Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 3 (118)/2003

Профили защиты на основе «Общих критериев»

Аналитический обзор

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Профили защиты на основе «Общих критериев»

Аналитический обзор

В.Б. Бетелин член-корреспондент РАН, В.А. Галатенко,
М.Т. Кобзарь, А.А. Сидак,
И.А. Трифаленков

СОДЕРЖАНИЕ

0. Аннотация

В статье анализируются профили защиты и их проекты, построенные на основе международного стандарта ISO/IEC 15408, описывающие сервисы безопасности, их комбинации и приложения. Выделяются общие требования, которые могут войти в состав функционального пакета, применимого ко всем сервисам, упрощающего разработку и понимание профилей для конкретных сервисов. Анализ профилей защиты позволяет оценить сильные и слабые стороны «Общих критериев», наметить возможные направления новых исследований.

1. Введение

В 1990 году под эгидой Международной организации по стандартизации (ИСО) были развернуты работы по созданию стандарта в области оценки безопасности информационных технологий (ИТ). Разработка этого стандарта преследовала следующие основные цели:

- унификация национальных стандартов в области оценки безопасности ИТ;
- повышение уровня доверия к оценке безопасности ИТ;
- сокращение затрат на оценку безопасности ИТ на основе взаимного признания сертификатов.

В июне 1993г. организации по стандартизации и обеспечению безопасности США, Канады, Великобритании, Франции, Германии и Нидерландов объединили свои усилия в рамках проекта по созданию единой совокупности критериев оценки безопасности ИТ. Этот проект получил название "Общие критерии" (ОК).

Общие критерии были призваны обеспечить взаимное признание результатов стандартизованной оценки безопасности на мировом рынке ИТ.

Разработка версии 1.0 «Общих критериев» (ОК) была завершена в январе 1996 года и одобрена ИСО в апреле 1996 года. Был проведен ряд экспериментальных оценок на основе версии 1.0 ОК, а также организовано широкое обсуждение документа.

В мае 1998 года была опубликована версия 2.0 ОК, и на ее основе в июне 1999 года принят международный стандарт ИСО/МЭК 15408. Официальный текст стандарта издан 1 декабря 1999 года [1-3]. Изменения, внесенные в стандарт на завершающей стадии его принятия, учтены в версии 2.1 ОК, идентичной стандарту по содержанию.

Уже после принятия стандарта с учетом опыта его использования появился ряд интерпретаций ОК, которые после рассмотрения специальным Комитетом по интерпретациям (CCIMB) принимаются, официально публикуются и вступают в силу как действующие изменения и дополнения к ОК. Параллельно с учетом интерпретаций ведется разработка версии 3.0 ОК.

Параллельное существование стандарта ISO (для которых существует пятилетний цикл обновления) и ОК с действующими интерпретациями дает возможность гибко и оперативно реагировать на необходимые уточнения и полезные для практики изменения ОК, которые впоследствии включаются в новую версию ОК и новую редакцию соответствующего стандарта.

В России Центром безопасности информации (ЦБИ), Центром «Атомзащитаинформ», ЦНИИАТОМИНФОРМ, ВНИИстандарт при участии экспертов Международной рабочей группы по Общим критериям был подготовлен проект ГОСТ Р ИСО/МЭК 15408, содержащий полный аутентичный текст международного стандарта. Стандарт [4-6] принят постановлением Госстандарта России от 4.04.2002 года № 133-ст с датой введения в действие 1 января 2004 года.

Для практической апробации ОК и нормативно-методических документов, разработанных в их поддержку [9,10], до ввода в действие ГОСТ Р ИСО/МЭК 15408 принят и введен в действие с 19.06.2002 года руководящий документ Гостехкомиссии России [7], полностью соответствующий указанному ГОСТ.

Международный стандарт ISO/IEC 15408, а также его российский вариант ГОСТ Р ИСО/МЭК 15408 «Критерии оценки безопасности информационных технологий» в применении к оценке безопасности изделий информационных технологий (ИТ) являются по сути метасредствами, задающими систему понятий, в терминах которых должна производиться оценка, и содержащими относительно полный каталог требований безопасности (функциональных и доверия), но не предоставляющих конкретных наборов требований и критериев для тех или иных типов продуктов и систем ИТ, выполнение которых необходимо проверять. Эти требования и критерии фигурируют в профилях защиты (ПЗ) и заданиях по безопасности (ЗБ). Предполагается, что профили защиты, в отличие от заданий по безопасности, носят относительно универсальный

характер: они характеризуют определенный класс изделий ИТ вне зависимости от специфики условий применения.

Именно официально принятые профили защиты образуют построенную на основе «Общих критериев» (ОК) и используемую на практике нормативную базу в области информационной безопасности (ИБ).

В настоящее время такая база и в мире (см., например, [11, 12]), и в России только создается. В России эту работу курирует Государственная техническая комиссия при Президенте РФ (Гостехкомиссия России). Представляется, что анализ разрабатываемых профилей, произведенный на относительно ранней стадии, является вполне своевременным и, более того, весьма важным, поскольку позволяет выявить только намечающиеся тенденции, взять на вооружение положительный опыт и попытаться избежать типичных ошибок.

Вообще говоря, профили защиты могут характеризовать отдельные сервисы безопасности, комбинации подобных сервисов, реализованные, например, в операционной системе, а также прикладные изделия ИТ, для которых обеспечение информационной безопасности критически важно (пример — смарт-карты).

Нас в первую очередь будут интересовать профили защиты сервисов безопасности, поскольку последние являются универсальными строительными блоками, позволяющими формировать защитные рубежи информационных систем (ИС) различного назначения, разной степени критичности. В работах В.Б. Бетелина и В.А. Галатенко (см., например, [13]) были выделены следующие базовые сервисы безопасности:

- идентификация и аутентификация;
- управление доступом;
- протоколирование и аудит;
- шифрование;
- контроль целостности;
- экранирование;
- анализ защищенности;
- обеспечение отказоустойчивости;
- обеспечение безопасного восстановления;
- туннелирование;
- управление.

В силу разных причин не для всех перечисленных сервисов безопасности профили защиты разработаны или разрабатываются. Такие сервисы, как идентификация и аутентификация, управление доступом, традиционные протоколирование и аудит, отказоустойчивость и безопасное восстановление адекватно описываются соответствующими классами функциональных требований «Общих критериев», поэтому формировать на их основе привычные классы защищенности относительно несложно (однако сделать это, разумеется, все же необходимо). Выделение сервисов туннелирования и управления в настоящее время не является общепринятым, поэтому пока они обойдены вниманием разработчиков ПЗ. Наконец, криптография во многих странах (да и в самих «Общих критериях») является «особой точкой» безопасности, так что создание профилей защиты для сервисов шифрования и контроля целостности затруднено по законодательным и/или организационным причинам. (Заметим в скобках, что хотя сложившееся вокруг компьютерной криптографии положение можно объяснить, его никак нельзя признать нормальным.). Далее основное внимание будет уделено оставшимся базовым, а также производным сервисам (таким, например, как виртуальные частные сети).

2. Общие требования к сервисам безопасности

Если придерживаться объектно-ориентированного подхода, то целесообразно выделить, по крайней мере, два уровня в иерархии наследования требований к сервисам безопасности:

- общие требования, применимые ко всем или многим сервисам;
- частные требования, специфичные для конкретного сервиса.

С точки зрения технологии программирования «Общие критерии» построены по дообъектной, «библиотечной» методологии. Они предоставляют параметризованные функциональные требования, но не содержат необходимые с практической точки зрения комбинации таких требований или универсальные интерфейсы, допускающие конкретизацию в контексте различных сервисов. Тем не менее, мы попытаемся выделить из разных профилей общие требования к сервисам безопасности, поскольку это упростит охват и понимание всей системы имеющихся профилей защиты.

2.1. Общие предположения безопасности

Предположения безопасности являются частью описания среды, в которой функционирует объект оценки. Можно выделить следующие общие предположения.

- Использование сервиса безопасности предусматривает наличие уполномоченного пользователя, выполняющего роль администратора, обладающего достаточной квалификацией, отвечающего за нормальное функционирование, осуществляющего сопровождение сервиса и действующего в соответствии с положениями политики безопасности.
- Предусматривается возможность удаленного администрирования сервиса.
- Политика управления атрибутами пользователей, например, данными аутентификации, проводится в жизнь, так что пользователи должным образом меняют эти данные с требуемой регулярностью.
- После того, как пользователя лишают доступа к сервису (например, в связи со сменой работы), его данные аутентификации и привилегии ликвидируются.
- Предусматривается резервное копирование информации, ассоциированной с сервисом (такой, например, как значения конфигурационных параметров).
- Аппаратно-программная среда сервиса безопасности является минимально достаточной для нормального функционирования.
- Предполагается физическая защищенность вычислительной установки, на которой функционирует сервис безопасности.
- Предполагается невозможность обхода сервиса безопасности.
- Предполагается, что вредоносный код не может иметь подпись доверенной стороны.
- Предполагается, что пользователи должным образом сообщают о случаях нарушения информационной безопасности.
- Предполагается, что пользователи и обслуживающий персонал способны противостоять методам морально-психологического воздействия.

С точки зрения проектирования объекта оценки, предположения безопасности, с одной стороны, являются условиями реализации сервисов безопасности, с другой стороны, определяют набор организационно-процедурных мер, ассоциированных с указанным сервисом.

2.2. Общие угрозы безопасности

Современные сервисы безопасности функционируют в распределенной среде, поэтому необходимо учитывать наличие как локальных, так и сетевых угроз. В качестве общих можно выделить следующие угрозы.

- Обход злоумышленником защитных средств.
- Осуществление злоумышленником физического доступа к вычислительной установке, на которой функционирует сервис безопасности.
- Ошибки администрирования, в частности, неправильная установка, ошибки при конфигурировании и т.п.
- Переход сервиса в небезопасное состояние в результате сбоя или отказа, при начальной загрузке, в процессе или после перезагрузки.
- Маскарад пользователя (попытка злоумышленника выдать себя за уполномоченного пользователя, в частности, за администратора). В распределенной среде маскарад может реализовываться путем подмены исходного адреса или воспроизведения ранее перехваченных данных идентификации/аутентификации.
- Маскарад сервера (попытка злоумышленника выдать свою систему за легальный сервер). Следствием маскарада сервера может стать навязывание пользователю ложной информации или получение от пользователя конфиденциальной информации.
- Использование злоумышленником чужого сетевого соединения или интерактивного сеанса (например, путем доступа к оставленному без присмотра терминалу).
- Несанкционированное изменение злоумышленником конфигурации сервиса и/или конфигурационных данных.
- Нарушение целостности программной конфигурации сервиса, в частности, внедрение троянских компонентов или получение контроля над сервисом.
- Несанкционированный доступ к конфиденциальной (например, регистрационной) информации, в том числе несанкционированное расшифрование зашифрованных данных.
- Несанкционированное изменение данных (например, регистрационной информации), в том числе таких, целостность которых защищена криптографическими методами.
- Несанкционированный доступ к данным (на чтение и/или изменение) в процессе их передачи по сети.

- Анализ потоков данных с целью получения конфиденциальной информации.
- Перенаправление потоков данных (в частности, на системы, контролируемые злоумышленником).
- Блокирование потоков данных.
- Повреждение или утрата регистрационной, конфигурационной или иной информации, влияющей на безопасность функционирования сервиса (например, из-за повреждения носителей или переполнения регистрационного журнала).
- Агрессивное потребление злоумышленником ресурсов, в частности, ресурсов протоколирования и аудита, а также полосы пропускания.
- Сохранение остаточной информации в многократно используемых объектах.

Хотя угрозы безопасности не должны в обязательном порядке делиться на угрозы для среды и угрозы для объекта оценивания, проведение такого разделения при разработке профиля оказывается полезным, поскольку делает формулировку целей безопасности (см. ниже) более логичной.

2.3. Общие элементы политики безопасности

Общие положения политики безопасности организации, относящиеся к защитным сервисам, могут состоять в следующем.

- Описания правил идентификации и аутентификации всех субъектов доступа (порядок аутентификации, разделение функций пользователя и администратора, условия, накладываемые на порядок аутентификации в зависимости от статуса и условий работы пользователя в информационной системе).
- Описания управления доступом к информационным ресурсам сервиса безопасности (модель доступа, критерии предоставления доступа, наборы привилегий субъектов доступа, порядок изменения правил доступа).
- Описание подотчетности пользователей, реализуемой посредством сервиса безопасности (какие действия пользователей при работе с какими сервисами могут быть подотчетны при применении объекта оценки, описанного в профиле).
- Описания правил протоколирования и аудита для анализа функционирования сервиса безопасности.
- Обеспечение доступности коммуникационных каналов.
- Описания правил обеспечения конфиденциальности и целостности управляющей информации (в частности, при удаленном администрировании).
- Описания порядка обеспечения целостности аппаратно-программной и информационной частей сервиса безопасности (список контролируемых компонент, порядок контроля и т.д.).
- Обеспечение невозможности обхода защитных средств (набор управленческих решений, обеспечивающих соответствующие предположения безопасности).

2.4. Общие цели безопасности для объекта оценки

Цели безопасности должны быть такими, чтобы их достижение позволяло противостоять угрозам безопасности и реализовать предписания политики безопасности. Общими для различных сервисов безопасности являются следующие цели.

- Подотчетность субъектов и объектов, взаимодействующих с сервисом.
  (Необходимым условием достижения этой цели является идентификация и аутентификация взаимодействующих субъектов и объектов, а также протоколирование и аудит выполняемых действий).
- Автоматизация административных действий, наличие средств проверки корректности конфигурации, как локальной, так и распределенной, наглядный интерфейс администрирования.
- Обеспечение (в первую очередь средствами пользовательского интерфейса) корректного использования функций безопасности.
- Предоставление пользователям средств для проверки аутентичности серверов и других партнеров по общению, а также открытых криптографических ключей. Проведение в жизнь подобных проверок.
- Выявление попыток нарушения политики безопасности, задание реакции на подобные попытки.
- Обеспечение отсутствия вредоносного кода в составе сервиса, в том числе после ликвидации нарушений информационной безопасности.
- Проверка программного кода на наличие подписи доверенной стороны перед загрузкой кода в систему.
- Выполнение резервного копирования информации, необходимой для восстановления нормальной работы сервиса.
- Обеспечение безопасного восстановления после сбоев и отказов.

- Обеспечение конфиденциальности и целостности информации при удаленном администрировании сервиса.
- Обеспечение устойчивости средств идентификации и аутентификации к попыткам воспроизведения информации и другим способам реализации маскарада.
- Наличие средств разграничения доступа к компонентам и ресурсам сервиса безопасности.
- Наличие средств контроля целостности компонентов и ресурсов сервиса.
- Наличие средств контроля корректности функционирования сервиса.
- Обеспечение безопасности многократного использования объектов.

2.5. Общие цели безопасности для среды

Цели безопасности для среды дополняют цели безопасности объекта оценки и состоят в следующем.

- Обеспечение минимальной достаточности аппаратной и программной конфигурации вычислительной установки, на которой функционирует сервис безопасности.
- Управление физическим доступом к компонентам и ресурсам сервиса.
- Обеспечение невозможности обхода защитных средств.
- Обеспечение достаточной подготовки уполномоченных пользователей сервиса безопасности.
- Проведение в жизнь политики управления данными аутентификации, так что пользователи должным образом меняют эти данные с требуемой регулярностью.
- Ликвидация данных аутентификации и привилегий пользователей, лишенных доступа к сервису безопасности.
- Разработка и реализация процедур и механизмов, предохраняющих от вторжения вредоносного ПО.
- Разработка и реализация дисциплины доклада о нарушениях информационной безопасности.
- Подготовка пользователей и обслуживающего персонала для противостояния методам морально-психологического воздействия.
- Оперативная ликвидация выявленных уязвимостей.

2.6. Общие функциональные требования

Для различных сервисов безопасности общими являются функциональные требования, связанные с идентификацией и аутентификацией, управлением доступом, протоколированием и аудитом, а также обеспечением высокой доступности. Далее эти требования разбиты в соответствии с иерархией, принятой в «Общих критериях».

2.6.1. Класс FAU: Аудит безопасности

Для сервисов безопасности предусматриваются следующие требования по протоколированию и аудиту.

- Автоматическая реакция аудита безопасности (FAU_ARP.1.1), например, генерация записи в регистрационном журнале, локальная или удаленная сигнализация администратору об обнаружении вероятного нарушения безопасности.
- Генерация данных аудита безопасности (FAU_GEN.1). Подлежат протоколированию, по крайней мере, запуск и завершение регистрационных функций, а также все события для базового уровня аудита. В каждой регистрационной записи должны присутствовать дата и время события, тип события, идентификатор субъекта и результат (успех или неудача) события.
- Анализ аудита безопасности (FAU_SAA.1.2). С целью выявления вероятных нарушений должны производиться, по крайней мере, накопление и/или объединение неуспешных результатов использования механизмов аутентификации, а также неуспешных результатов выполнения криптографических операций.
- Просмотр аудита безопасности (FAU_SAR). Администратору предоставляется возможность читать всю регистрационную информацию. Прочим пользователям доступ к регистрационной информации закрыт, за исключением явно специфицированных случаев.
- Выбор событий аудита безопасности (FAU_SEL.1). Избирательность регистрации событий должна основываться, по крайней мере, на следующих атрибутах: идентификатор объекта, идентификатор субъекта, адрес узла сети, тип события, дата и время события.
- Хранение данных аудита безопасности (FAU_STG.1.2). Регистрационная информация должна быть защищена от несанкционированной модификации.

2.6.2. Класс FCS: Криптографическая поддержка

Многие сервисы безопасности прямо или косвенно нуждаются в криптографической поддержке, поэтому соответствующие требования целесообразно трактовать как общие.

- Управление криптографическими ключами (FCS_CKM). Должны поддерживаться генерация криптографических ключей (FCS_CKM.1), распределение криптографических ключей

(FCS_CKM.2), управление доступом к криптографическим ключам (FCS_CKM.3), уничтожение криптографических ключей (FCS_CKM.4).
- Криптографические операции (FCS_COP.1). Для всей информации, передаваемой по доверенному каналу, должны осуществляться шифрование и контроль целостности в соответствии с требованиями стандартов и других нормативных документов.

2.6.3. Класс FDP: Защита данных пользователя

Любой сервис безопасности содержит данные пользователей (например, информацию для идентификации и аутентификации), поэтому следующие требования являются общими.
- Политика управления доступом (FDP_ACC.1.1). Должно осуществляться разграничение доступа для пользователей, прямо или косвенно выполняющих операции с сервисом безопасности.
- Функции управления доступом (FDP_ACF.1.1). Применение функций разграничения доступа должно основываться, по крайней мере, на следующих атрибутах безопасности: идентификаторы субъектов доступа, идентификаторы объектов доступа, адреса субъектов доступа, адреса объектов доступа, права доступа субъектов.
- Базовая защита внутренней передачи (FDP_ITT.1). Должна осуществляться заданная политика управления доступом и/или информационными потоками, чтобы предотвратить раскрытие, модификацию и/или недоступность данных пользователя при их передаче между физически разделенными частями сервиса безопасности (FDP_ITT.1.1).
- Защита остаточной информации (FDP_RIP.2.1). Для всех объектов должна обеспечиваться полная защита остаточной информации, то есть недоступность предыдущего состояния при освобождении ресурса.

2.6.4. Класс FIA: Идентификация и аутентификация

Необходимость идентификации и аутентификации пользователей сервисов безопасности является следствием общего требования подотчетности.
- Отказы аутентификации (FIA_AFL.1.2). При достижении определенного администратором числа неуспешных попыток аутентификации необходимо отказать субъекту в доступе, сгенерировать запись регистрационного журнала и сигнализировать администратору о вероятном нарушении безопасности.
- Определение атрибутов пользователя (FIA_ATD.1.1). Для каждого пользователя необходимо поддерживать, по крайней мере, следующие атрибуты безопасности:
идентификатор, аутентификационная информация (например, пароль), права доступа (роль). В частности, если аутентификационная информация обеспечивается криптографическими операциями, должны поддерживаться также открытые и секретные ключи.
- Идентификация (FIA_UID) и аутентификация (FIA_UAU) пользователя. Каждый пользователь должен быть успешно идентифицирован (FIA_UID.2.1) и аутентифицирован (FIA_UAU.2.1) до разрешения любого действия, выполняемого сервисом безопасности от имени этого пользователя. Необходимо предотвращать применение аутентификационных данных, которые были подделаны или скопированы у другого пользователя (FIA_UAU.3). Следует аутентифицировать любой представленный идентификатор пользователя (FIA_UAU.5.2). Необходимо повторно аутентифицировать пользователя по истечении определенного администратором интервала времени (FIA_UAU.6.1). Функции безопасности должны предоставлять пользователю только скрытую обратную связь во время выполнения аутентификации (FIA_UAU.7).
- Связывание пользователь-субъект (FIA_USB.1.1). Следует ассоциировать соответствующие атрибуты безопасности пользователя с субъектами, действующими от имени этого пользователя.

2.6.5. Класс FMT: Управление безопасностью

Управление — важнейший аспект информационной безопасности, а требования управления, несомненно, принадлежат к числу общих.
- Управление отдельными функциями безопасности (FMT_MOF.1.1). Только администратор должен иметь возможность определения режима функционирования, отключения, подключения, модификации режимов идентификации и аутентификации, управления правами доступа, протоколирования и аудита.
- Управление атрибутами безопасности (FMT_MSA). Только администратор должен иметь возможность изменения подразумеваемых значений, опроса, изменения, удаления, создания атрибутов безопасности, правил управления потоками информации (FMT_MSA.1.1). Следует обеспечить присваивание атрибутам безопасности только безопасных значений (FMT_MSA.2.1).
- Управление данными функций безопасности (FMT_MTD). Только администратор должен

иметь возможность изменения подразумеваемых значений, опроса, изменения, удаления, очистки, определения типов регистрируемых событий, размеров регистрационных журналов, прав доступа субъектов, сроков действия учетных записей субъектов доступа, паролей, криптографических ключей (FMT_MTD.1.1).

Только администратор должен иметь возможность определения ограничений размеров регистрационных журналов, сроков действия учетных записей субъектов доступа, паролей, криптографических ключей, числа неудачных попыток аутентификации, интервалов бездействия пользователей (FMT_MTD.2.1). При выходе за допустимые границы должны выполняться определенные администратором действия, такие как сигнализация администратору, блокирование или удаление учетной записи, запрос на смену пароля или ключа и т.д. (FMT_MTD.2.2). Следует обеспечить присваивание данным функций безопасности только безопасных значений (FMT_MTD.3.1).

- Отмена (FMT_REV.1). Только у уполномоченных администраторов должна быть возможность отмены атрибутов безопасности, ассоциированных с пользователями.
  Важные для безопасности полномочия должны отменяться немедленно (FMT_REV.1.2).
- Роли управления безопасностью (FMT_SMR). Должны поддерживаться, по крайней мере, следующие роли: уполномоченный пользователь, удаленный пользователь, администратор (FMT_SMR.1.1). Получение ролей удаленного пользователя и администратора может производиться только по явному запросу (FMT_SMR.3.1).

Термин «администратор» в данном случае определяет одного пользователя или группу пользователей, наделенных соответствующими правами. Естественно, при работе группы администраторов их полномочия разделяются в соответствии с принципом минимизации привилегий, и реализация этого разделения должна быть явно указана для объекта оценки.

Необходимо также отметить, что описанные выше функции администратора должны быть сформулированы также как требования политики безопасности, поскольку администратор, вообще говоря, лишь реализует указанную политику. Прав на прочие действия у него не должно быть.

2.6.6. Класс FPR: Приватность

Приватность — специфический аспект информационной безопасности, однако требование открытости для уполномоченного пользователя носит общий характер.

- Скрытность (FPR_UNO). Администратор должен иметь возможность наблюдать за использованием ресурсов сервиса безопасности (FPR_UNO.4.1).

2.6.7. Класс FPT: Защита функций безопасности

Собственная защищенность — важная характеристика любого сервиса безопасности. В число общих входят следующие требования.

- Тестирование абстрактной машины (FPT_AMT.1). Для демонстрации выполнения предположений безопасности, обеспечиваемых абстрактной машиной, положенной в основу сервиса безопасности, при запуске и/или по запросу администратора должен выполняться пакет тестовых программ (FPT_AMT.1.1).
- Безопасность при сбое (FPT_FLS). Сервис должен сохранять безопасное состояние при аппаратных сбоях (вызванных, например, перебоями электропитания) (FPT_FLS.1.1).
- Целостность экспортируемых данных (FPT_ITI). Сервис должен предоставлять возможность верифицировать целостность всех данных при их передаче между ним и удаленным доверенным изделием ИТ и выполнять повторную передачу информации, а также генерировать запись регистрационного журнала, если модификации обнаружены (FPT_ITI.1.2).
- Надежное восстановление (FPT_RCV). Когда автоматическое восстановление после сбоя или прерывания обслуживания невозможно, сервис должен перейти в режим аварийной поддержки, позволяющей вернуться к безопасному состоянию (FPT_RCV.2.1). После аппаратных сбоев должен обеспечиваться возврат к безопасному состоянию с использованием автоматических процедур (FPT_RCV.2.2).
- Обнаружение повторного использования (FPT_RPL). Сервис должен обнаруживать повторное использование аутентификационных данных (FPT_RPL.1.1), отказать в доступе, сгенерировать запись регистрационного журнала и сигнализировать администратору о вероятном нарушении безопасности (FPT_RPL.1.2).
- Посредничество при обращениях (FPT_RVM). Функции, осуществляющие политику безопасности сервиса, должны вызываться и успешно выполняться прежде, чем разрешается выполнение любой другой функции сервиса (FPT_RVM.1.1). Компонент FPT_RVM.1 направлен на обеспечение невозможности обхода защитных средств.

- Разделение доменов (FPT_SEP). Функции безопасности должны поддерживать отдельный домен для собственного выполнения, который защищает их от вмешательства и искажения недоверенными субъектами (FPT_SEP.1.1).
- Метки времени (FPT_STM). Для использования функциями безопасности должны предоставляться надежные метки времени (FPT_STM.1.1).
- Согласованность данных между функциями безопасности (FPT_TDC). Должна обеспечиваться согласованная интерпретация регистрационной информации, а также параметров используемых криптографических операций (FPT_TDC.1.1).
- Согласованность данных функций безопасности при дублировании в пределах объекта оценки (FPT_TRC). Должна обеспечиваться согласованность данных функций безопасности при дублировании их в различных частях объекта оценки (FPT_TRC.1.1). Когда части, содержащие дублируемые данные, разъединены, согласованность должна обеспечиваться после восстановления соединения перед обработкой любых запросов к заданным функциям безопасности (FPT_TRC.1.2).
- Самотестирование функций безопасности (FPT_TST). Для демонстрации правильности работы функций безопасности при запуске, периодически в процессе нормального функционирования и/или по запросу администратора должен выполняться пакет программ самотестирования (FPT_TST.1.1). У администратора должна быть возможность верифицировать целостность данных (FPT_TST.1.2) и выполняемого кода функций безопасности (FPT_TST.1.3).

2.6.8. Класс FTA: Доступ к объекту оценки

Требования данного класса направлены на обеспечение защищенности от агрессивного потребления ресурсов.

- Ограничение на параллельные сеансы (FTA_MCS). Должно ограничиваться максимальное число параллельных сеансов, предоставляемых одному пользователю (FTA_MCS.1.1). У этой величины должно быть подразумеваемое значение, устанавливаемое администратором (FTA_MCS.1.2).
- Блокирование сеанса (FTA_SSL). По истечении установленного администратором значения длительности бездействия пользователя сеанс работы должен принудительно завершаться (FTA_SSL.3.1).
- Открытие сеанса с объектом оценки (FTA_TSE). Сервис должен быть способен отказать в открытии сеанса, основываясь на идентификаторе субъекта, пароле субъекта, правах доступа субъекта (FTA_TSE.1.1).

2.6.9. Класс FTP: Доверенный маршрут/канал

Обеспечение защищенного взаимодействия сервисов безопасности в распределенной среде — одно из важнейших общих требований.

- Доверенный канал передачи между функциями безопасности (FTP_ITC). Для связи с удаленным доверенным изделием ИТ функции безопасности должны предоставлять канал, который логически отличим от других и обеспечивает надежную аутентификацию его сторон, а также защиту данных от модификации и раскрытия (FTP_ITC.1.1). У обеих сторон должна быть возможность инициирования связи через доверенный канал (FTP_ITC.1.2, FTP_ITC.1.3).
- Доверенный маршрут (FTP_TRP). Для связи с удаленным пользователем функции безопасности должны предоставлять маршрут, который логически отличим от других и обеспечивает надежную аутентификацию его сторон, а также защиту данных от модификации и раскрытия (FTP_TRP.1.1). У пользователя должна быть возможность инициирования связи через доверенный маршрут (FTP_TRP.1.2). Для начальной аутентификации удаленного пользователя и удаленного управления использование доверенного маршрута является обязательным (FTP_TRP.1.3).

На этом мы завершаем изложение общих функциональных требований к сервисам безопасности.

2.7. Общие требования доверия безопасности

Требования доверия безопасности, по сравнению с функциональными, представляются более проработанными, поскольку для них определены удобные на практике оценочные уровни доверия (ОУД).

Для большинства областей применения достаточно третьего уровня доверия; с другой стороны, этот уровень достижим при разумных затратах на разработку, так что его можно считать типовым.

В число требований доверия третьего оценочного уровня входят:

- анализ функциональной спецификации, спецификации интерфейсов, эксплуатационной документации;
- независимое тестирование;
- наличие проекта верхнего уровня;
- анализ стойкости функций безопасности;
- поиск разработчиком явных уязвимостей;

- контроль среды разработки;
- управление конфигурацией.

В принципе достижим и четвертый оценочный уровень, который можно рекомендовать для конфигураций повышенной защищенности. В число дополнительных требований этого уровня входят:

- полная спецификация интерфейсов;
- наличие проектов нижнего уровня;
- анализ подмножества реализации;
- применение неформальной модели политики безопасности;
- независимый анализ уязвимостей;
- автоматизация управления конфигурацией.

Вероятно это самый высокий уровень, который можно достичь при существующей технологии программирования и разумных затратах материальных и временных ресурсов.

3. Специфические требования к сервисам безопасности

В данном разделе основное внимание будет уделено специфическим функциональным требованиям, как наиболее важным для обеспечения безопасности.

3.1. Управление доступом

3.1.1. Профиль защиты для дискреционного управления доступом

Дальнейшее изложение основано на первой редакции проекта [14] «Контролируемый доступ. Профиль защиты» (ПЗ КД), подготовленного в Центре безопасности информации. Его прототип [15], базирующийся на версии 2.0 «Общих критериев», был подготовлен в 1999 году в Агентстве национальной безопасности США и лег в основу сертификации многих продуктов ИТ, в том числе операционной системы Windows 2000.

В принципе ПЗ КД соответствует классу безопасности С2 «Оранжевой книги» [16] или пятому классу защищенности по классификации Гостехкомиссии России для средств вычислительной техники [17], однако применение методологии и обширного набора требования безопасности из «Общих критериев» позволило сделать профиль, по сравнению с упомянутыми документами, существенно более детальным и обоснованным.

Из соответствия классу безопасности С2 следует, что в ПЗ КД рассматривается только дискреционное (произвольное) управление доступом. Требования, включенные в профиль, направлены на достижение базового уровня безопасности в условиях невраждебного и хорошо управляемого сообщества пользователей, при наличии лишь непреднамеренных угроз.

Из числа специфических функциональных требований ПЗ КД выделим следующие.

- Ассоциация идентификатора пользователя (FAU_GEN.2). Функции безопасности должны ассоциировать каждое потенциально протоколируемое событие с идентификатором пользователя — инициатора этого события. (На первый взгляд кажется, что у данного требования есть очевидные исключения, например, неудачные попытки идентификации/аутентификации, однако на этой стадии средства контролируемого доступа еще не используются, а за идентификацию и аутентификацию отвечает другой сервис безопасности).
- Выборочный просмотр аудита (FAU_SAR.3). Должна предоставляться возможность поиска, сортировки, упорядочения регистрационных данных, основываясь на идентификаторах пользователей и, быть может, других специфицированных атрибутах.
- Управление доступом, основанное на атрибутах безопасности (FDP_ACF.1). Проводимая политика дискреционного управления доступом должна основываться на таких атрибутах, как идентификатор пользователя и принадлежность к группе (группам), а также атрибутах, ассоциированных с объектами. Последние дают возможность сопоставления разрешенных и запрещенных операций с идентификаторами одного или более пользователей и/или групп, задания разрешенных или запрещенных по умолчанию операций.
- Определение атрибутов пользователя (FIA_ATD.1). Для каждого пользователя должен поддерживаться следующий список атрибутов безопасности: идентификатор пользователя, принадлежность к группе, данные аутентификации, допустимые роли.
- Верификация секретов (FIA_SOS.1). При попытке использования механизма аутентифика-

ции вероятность того, что произойдет случайный доступ, должна быть меньше, чем 1:1000000. При неоднократных попытках использования механизма аутентификации в течение одной минуты, вероятность того, что произойдет случайный доступ, должна быть меньше, чем 1:1000000. Любая обратная связь при попытках использования механизма аутентификации не должна приводить к превышению указанного уровня вероятности.

- Связывание пользователь-субъект (FIA_USB.1). Функции безопасности должны ассоциировать следующие атрибуты безопасности пользователя с субъектами, действующими от имени этого пользователя: идентификатор пользователя, который ассоциируется с событиями аудита; идентификаторы пользователя, используемые для осуществления политики дискреционного управления доступом; принадлежность к группам, используемая для осуществления политики дискреционного управления доступом.
- Инициализация статических атрибутов (FMT_MSA.3). Должны обеспечиваться ограничительные подразумеваемые значения для атрибутов безопасности, которые используются для осуществления политики дискреционного управления доступом (FMT_MSA.3.1). Должна предоставляться возможность определять альтернативные начальные значения для отмены подразумеваемых значений при создании объектов (FMT_MSA.3.2).
- Отмена (FMT_REV.1). Возможность отмены атрибутов безопасности, ассоциированных с объектами, должна предоставляться только пользователям, уполномоченным на это политикой дискреционного управления доступом (FMT_REV.1.1).

Рассмотренный профиль показывает, что выделение общих требований к сервисам безопасности значительно сокращает специфическую часть, облегчает ее изучение и верификацию.

3.1.2. Профиль защиты для мандатного управления доступом

В данном подразделе рассматривается первая редакция проекта [18] «Меточная защита. Профиль защиты» (ПЗ МЗ), подготовленного в Центре безопасности информации (см. также [19]). ПЗ МЗ соответствует классу безопасности B1 «Оранжевой книги» [16] или четвертому классу защищенности по классификации Гостехкомиссии России для средств вычислительной техники [17].

Профиль защиты для мандатного (принудительного) управления доступом имеет много общего с рассмотренным в предыдущем подразделе профилем ПЗ КД. Некоторые отличия носят очевидный характер (например, включение меток безопасности в записи регистрационного журнала (семейство функциональных требований FAU_GEN), выборочный просмотр аудита на основании меток безопасности (FAU_SAR) или включение в число атрибутов безопасности пользователя данных о допуске (FIA_ATD)). Ни на общих свойствах этих двух профилей, ни на рутинных отличиях мы останавливаться не будем.

Специфическими для ПЗ МЗ являются следующие функциональные требования.

- Экспорт данных пользователя (FDP_ETC). При экспорте назначенных данных пользователя должна осуществляться политика мандатного управления доступом (FDP_ETC.1.1, FDP_ETC.2.1). Непомеченные данные должны экспортироваться без атрибутов безопасности (FDP_ETC.1.2), помеченные — с однозначно ассоциированными атрибутами (FDP_ETC.2.2, FDP_ETC.2.3). Устройства, используемые для экспорта данных без атрибутов безопасности, не могут использоваться для экспорта с атрибутами за исключением ситуации, когда изменение в состоянии устройства выполнено вручную и может быть запротоколировано (FDP_ETC.2.4). (Отметим, что в ОК в компоненте FDP_ETC.1 отсутствует элемент, необходимый для назначения правил управления экспортом непомеченных данных).
- Ограниченное управление информационными потоками (FDP_IFC.1). Для назначенных субъектов и объектов и всех операций над этими субъектами и объектами должна осуществляться политика мандатного управления доступом (FDP_IFC.1.1).
- Иерархические атрибуты безопасности (FDP_IFF.2). Политика мандатного управления доступом должна основываться на метках безопасности субъектов и объектов (FDP_IFF.2.1). Метка безопасности должна состоять из иерархического уровня и набора неиерархических категорий. На множестве допустимых меток безопасности должно быть определено отношение частичного порядка со следующими свойствами (FDP_IFF.2.7). Метки равны, если совпадают их уровни и наборы категорий. Метка A больше метки B, если: уровень A больше уровня B и набор категорий B является подмножеством набора A; уровень A равен уровню B и набор категорий B является собственным подмножеством набора A. Метки несравнимы, если они не равны и ни одна из меток не больше другой. Для любых двух допустимых меток су-

ществует наименьшая верхняя грань, которая больше или равна этим меткам, а также наибольшая нижняя грань, которая не больше обеих меток. Должно поддерживаться, по крайней мере, 16 уровней и 64 категории. Информационный поток между управляемыми субъектами и объектами посредством управляемой операции разрешен, если метка источника больше или равна метке целевого субъекта или объекта (FDP_IFF.2.2).
- Импорт данных пользователя (FDP_ITC). Это семейство требований симметрично экспортным требованиям FDP_ETC.
- Управление атрибутами безопасности (FMT_MSA.1). Функции безопасности должны осуществлять политику мандатного управления доступом, чтобы ограничить право модификации меток безопасности, ассоциированных с объектами.
- Роли безопасности (FMT_SMR.1). В число поддерживаемых должна входить роль, дающая право изменять атрибуты безопасности объектов.

Для требований доверия безопасности рассматриваемым профилем предписан оценочный уровень 3, усиленный компонентом ADV_SPM.1 (неформальная модель политики безопасности объекта оценки).

3.1.3. Ролевое управление доступом

Ролевое управление доступом (Role-Based Access Control, RBAC) представляет собой универсальный каркас, нейтральный по отношению к конкретной дисциплине разграничения доступа и предназначенный в первую очередь для упрощения администрирования информационных систем с большим числом пользователей и различных ресурсов.

Ниже рассматриваются специфические требования для профиля RBAC [20, 21], основанного на версии 2.0 «Общих критериев».

Разделение обязанностей — существенная и специфичная для ролевого управления доступом цель безопасности. Возможность ее достижения — важное достоинство ролевого доступа.

Еще одна специфическая и методологически важная цель безопасности — организация иерархии ролей с наследованием прав доступа. Применение идей и методов объектно-ориентированного подхода необходимо для успешной работы с большими системами.

Функциями, специфичными для ролевого управления доступом, являются:
- создание и удаление ролей, создание, удаление и модификация атрибутов ролей и отношений между ролями;
- формирование и поддержка ассоциаций между пользователями и ролями;
- формирование и поддержка ассоциаций между правами доступа и ролями.

Эти функции обслуживаются тремя классами функциональных требований, на которых мы и остановимся.
- Ограниченное управление доступом (FDP_ACC.1.1). По крайней мере для части операций субъектов над объектами должно действовать ролевое управление доступом, которое в общем случае может существовать с другими дисциплинами разграничения доступа.
- Управление доступом, основанное на атрибутах безопасности (FDP_ACF.1.1). В число учитываемых атрибутов безопасности должны входить, помимо прочих, присвоенные субъекту роли и права доступа этих ролей.
- Управление данными функций безопасности (FMT_MTD). Только администратор должен иметь возможность определения и изменения ролей, их атрибутов, связей между ними и ограничений на подобные связи (FMT_MTD.1.1). Необходимы и другие требования класса FMT, но они в данном случае носят прямолинейный характер и рассматриваться не будут.
- Безопасность при сбое (FPT_FLS). Должно сохраняться безопасное состояние в ситуациях, когда база данных ролей недоступна или повреждена (FPT_FLS.1.1). Как и в случае управления безопасностью, другие требования этого класса необходимы, но не нуждаются в детальном рассмотрении.

Можно видеть, что функциональные требования «Общих критериев» полезны для достижения тактических целей безопасности. Стратегические цели, носящие концептуальный или архитектурный характер, такие как организация иерархии ролей с небольшим числом сущностей на каждом уровне или следование принципу разделения обязанностей, приходится формулировать отдельно, без стандартизованной понятийной базы.

3.2. Межсетевые экраны

Для межсетевых экранов (МЭ) разработан целый ряд профилей защиты и проектов таких профилей (см. [22-26]). Отметим, что экранирование — это, видимо, единственный сервис безопасности, для которого Гостехкомиссия России одной из первых в мире разработала и ввела в действие Руководящий документ [27], основные идеи которого получили международное признание и фигурируют в профилях

защиты, имеющих официальный статус в таких странах, как США.

Межсетевые экраны классифицируются на основании уровней эталонной семиуровневой модели, на которых осуществляется фильтрация потоков данных.

3.2.1. Пакетная фильтрация

Дальнейшее изложение основывается на профиле [24], как наиболее представительном среди документов аналогичного назначения.

В общем случае рассматривается многокомпонентный межсетевой экран. Политика безопасности МЭ базируется на принципе «все, что не разрешено, запрещено».

Информация, поступающая в МЭ, может предназначаться для фильтрации или для изменения параметров самого МЭ. В первом случае идентификация/аутентификация не требуется, во втором она является обязательной, причем должны использоваться одноразовые пароли (идентифицироваться и аутентифицироваться должны как операторы, осуществляющие удаленное администрирование, так и устройства, такие как маршрутизаторы, посылающие информацию для МЭ, например, измененные таблицы маршрутизации). Для формального описания перечисленных требований используются компоненты FMT_MSA.1 (управление атрибутами безопасности), FMT_MSA.3 (статическая инициализация атрибутов) и FIA_UAU.5 (сочетание механизмов аутентификации).

Поскольку «Общие критерии» не предназначены для оценки специфических качеств криптографических алгоритмов, рассматриваемый профиль ссылается на федеральный стандарт США FIPS PUB 140-1, требуя согласованности с ним для средств аутентификации, шифрования и контроля целостности. Формальной оболочкой для данного требования является компонент ОК FCS_COP.1.

Решения по фильтрации потоков данных принимаются на основе набора правил, в которых могут фигурировать исходный и целевой сетевые адреса, протокол транспортного уровня, исходный и целевой порты, а также входной и выходной сетевой интерфейс. Формально ограниченное управление информационными потоками между неаутентифицируемыми сущностями описывается компонентом FDP_IFC.1, а используемые при этом простые атрибуты безопасности — компонентом FDP_IFF.1.

Выборочный просмотр регистрационной информации (FAU_SAR.3.1) может основываться на адресах, диапазонах адресов, номерах портов, диапазонах дат и времени.

В плане требований доверия безопасности рассматриваемый профиль ограничивается оценочным уровнем 2, что, на наш взгляд, недостаточно для защиты критически важных систем, функционирующих в среде со средним уровнем риска.

Отметим, что за пределами рассмотрения в профиле остались такие технологические аспекты, как согласованность базы правил фильтрации для многокомпонентных конфигураций, удобство административного интерфейса (являющееся необходимым условием уменьшения числа ошибок администрирования), защита от атак на доступность.

Следует также отметить, что чисто пакетные фильтры практически никогда не являются собственно межсетевыми экранами (исключая может быть средства отечественного производства), а составляют часть ПО в операционных системах (как ip-chains в Linux) или специализированном ПО активного сетевого оборудования (как Cisco IOS).

3.2.2. Комплексное экранирование

Современные комплексные межсетевые экраны, осуществляющие фильтрацию на всех уровнях, включая прикладной, вообще говоря, по сравнению с пакетными фильтрами обеспечивают более надежную защиту, что нашло отражение в дополнительных требованиях безопасности, включенных в профили [22] и [25, 26].

В состав комплексных межсетевых экранов могут входить серверы-посредники, требующие идентификации и аутентификации (с помощью механизмов, основанных на данных одноразового использования и соответствующих компоненту FIA_UAU.4) пользователей соответствующих сетевых услуг (таких, например, как FTP или Telnet).

В правилах фильтрации могут фигурировать команды протоколов прикладного уровня и параметры команд.

В проекте профиля [25] требуется полное управление межсетевым доступом (компонент FDP_ACC.2), а также предотвращение угроз доступности (FDP_IFC.2.1).

Важным моментом проекта [25] являются требования анонимности (FPR_ANO.1.1), псевдонимности (FPR_PSE.1) и невозможности ассоциации (FPR_UNL.1.1) межсетевого доступа для сущностей, ассоциированных с защищаемой сетью или самим межсетевым экраном. Эти требования могут быть выполнены на основе использования механизма трансляции адресов и применения серверов-посредников.

Пример проекта [25] показывает, что в российских условиях можно обойти формальные, но не содержательные проблемы, связанные с криптографией. В любом случае криптографические аппа-

ратные и программные модули необходимо разрабатывать и/или оценивать, даже если само слово «криптография» в профиле защиты отсутствует.

Шифрование и контроль целостности необходимы для организации доверенного канала с целью обеспечения безопасности удаленного администрирования (соответствующие требования были рассмотрены ранее в числе общих для различных сервисов). Для них существуют российские ГОСТы, которыми можно воспользоваться при построении аналогов профилей [22] и [24]. Аутентификация, устойчивая к сетевым угрозам, также обязательна, однако для нее национальный криптографический ГОСТ отсутствует. Приходится, как это сделано в [25], ограничиваться общими требованиями верификации секретов (FIA_SOS.1) и защищенности от подделки (FIA_UAU.3). Впрочем, в любом случае привлечение национальных (а не международных) стандартов создает проблемы взаимодействия с иностранными партнерами и взаимного признания сертификатов разными странами.

3.3. Системы активного аудита

В работе [28] приведен набросок семейства профилей защиты для классификации систем активного аудита, а также соображения по расширению набора функциональных требований «Общих критериев». Проекты ПЗ для важнейших компонентов подобных систем — анализатора и сенсора — представлены в [29, 30].

Под подозрительной активностью понимается поведение пользователя или компонента информационной системы, являющееся злоумышленным (в соответствии с заранее определенной политикой безопасности) или нетипичным (согласно принятым критериям).

Назначение активного аудита — оперативно выявлять подозрительную активность и предоставлять средства для автоматического реагирования на нее.

По целому ряду причин, из числа которых мы выделим обеспечение масштабируемости, средства активного аудита строятся в архитектуре менеджер/агент. Основными агентскими компонентами являются компоненты извлечения регистрационной информации (сенсоры). Анализ, принятие решений — функции менеджеров. Очевидно, между менеджерами и агентами должны быть сформированы доверенные каналы.

В число функций безопасности, специфичных для средств активного аудита, входят генерация и извлечение регистрационной информации, ее анализ и реагирование на подозрительную активность.

Отметим, что такой универсальный аспект, как безопасное администрирование, для средств активного аудита приобретает особое значение, если включить в него автоматическую коррекцию (в первую очередь — пополнение) базы сигнатур атак. Тем не менее, соответствующие требования целесообразно отнести к числу общих, поскольку аналогичная возможность нужна, например, такому сервису безопасности, как анализ защищенности.

Из существенных для активного аудита компонентов класса FAU «Аудит безопасности» в «Общих критериях» отсутствуют анализ на соответствие политике безопасности (пороговый, статистический и сигнатурный анализы в семействе FAU_SAA предусмотрены), хранилища для описаний контролируемых объектов и для анализируемой информации, а также все интерфейсные компоненты. Слабо отражена возможность выбора рассматриваемых событий как сенсорами (агентами), так и анализаторами (менеджерами).

С целью адекватного отражения специфики средств активного аудита, в [28] предложен ряд добавлений к стандартному набору функциональных требований.

В семейство FAU_GEN (генерация данных аудита безопасности) предлагается включить два новых компонента.

FAU_GEN.3 — ассоциирование объекта, операция с которым вызвала событие, с включением в регистрационные записи имени (идентификатора) этого объекта. На минимальном уровне должны протоколироваться открытие/закрытие объекта (установление/разрыв соединения и т.п.), на базовом — все промежуточные операции. На детальном уровне в регистрационные записи должны входить все операнды операции с объектом.

Компонент FAU_GEN.3 добавлен по двум причинам. Во-первых, должна соблюдаться симметрия между субъектами и объектами. Во-вторых, статистические профили целесообразно строить не для субъектов, а для объектов, но для этого нужно располагать соответствующей информацией.

Еще один предлагаемый компонент — FAU_GEN.4 — предназначен для обеспечения неотказуемости сервиса, пользующегося услугами семейства FAU_GEN, от регистрации события. Вообще говоря, неотказуемость реализуется безотносительно к использованию коммуникаций, поэтому здесь нельзя воспользоваться классом FCO.

Стандартный компонент FAU_SAR.3 дает возможность осуществлять поиск и сортировку регистрационной информации, задавая в качестве критериев логические выражения.

Подобные выражения полезны также для задания фильтров, управляющих работой сенсоров.

Автоматический анализ регистрационной информации с целью выявления подозрительной активности представлен в «Общих критериях» четырьмя компонентами семейства FAU_SAA.

FAU_SAA.1 ориентирован на обнаружение превышения порогов, заданных фиксированным набором правил.

FAU_SAA.2 служит для выявления нетипичной активности путем анализа профилей поведения. В «Общих критериях» предлагаются профили для субъектов, хотя профили объектов могут оказаться предпочтительными. «Общие критерии» допускают анализ, как в реальном времени, так и постфактум. Поддержку анализа в реальном времени следует рассматривать как важнейшую отличительную особенность средств активного аудита.

FAU_SAA.3 направлен на выявление простых атак путем проведения сигнатурного анализа.

FAU_SAA.4 позволяет выявлять сложные, многоэтапные атаки, осуществляемые группой злоумышленников.

Предусматривается возможность настройки всех четырех компонентов путем добавления, модификации или удаления правил, отслеживаемых субъектов и сигнатур.

В [28] вводится еще один компонент, FAU_SAA.5, позволяющий выявлять нарушения политики безопасности. Задавать политики предлагается с помощью предикатов первого порядка.

В плане автоматического реагирования на подозрительную активность «Общие критерии» по сути ограничились констатацией подобной возможности. В [28] рассматривается более сложная сущность — решатель, который, получив рекомендации от компонентов анализа, определяет, действительно ли имеет место подозрительная активность, и, при необходимости, надлежащим образом реагирует (выбирая форму реакции в зависимости от серьезности выявленных нарушений).

Это значит, что решатель должен уметь:

- ранжировать подозрительную активность;
- реагировать в соответствии с рангом нарушения.

Оба аспекта должны управляться администратором безопасности.

В качестве отдельной возможности, присущей системам высокого класса, фигурирует проведение корреляционного анализа информации.

Описание контролируемых объектов и хранение соответствующей информации — важнейшая составная часть средств активного аудита, придающая им свойства расширяемости и настраиваемости. К этому компоненту предъявляются в первую очередь технологические требования.

Мониторы, как организующие оболочки для менеджеров средств активного аудита, должны обладать двумя группами свойств:

- обеспечивать защиту процессов, составляющих менеджер, от злоумышленных воздействий;
- обеспечивать высокую доступность этих процессов.

Первая группа обслуживается семейством FPT_SEP.

Вторая группа свойств может обеспечиваться такими техническими решениями, как программное обеспечение промежуточного слоя, кластерные конфигурации и т.д.

В плане безопасности целесообразно следовать требованиям FPT_FLS.1 (невозможность перехода в небезопасное состояние в случае сбоя или отказа), а также FPT_RCV.2, FPT_RCV.3, FPT_RCV.4 (надежное восстановление в автоматическом режиме, без потери данных, с точностью до функции безопасности).

Безопасность интерфейсов монитора (с другими мониторами, сенсорами, администратором безопасности) может обеспечиваться компонентами FPT_ITI.1, FPT_ITI.2 (обнаружение и исправление модификации экспортируемых данных), FPT_ITC.1 (конфиденциальность экспортируемых данных), FPT_ITA.1 (доступность экспортируемых данных).

На рабочем месте администратора безопасности должны быть обеспечены стандартные для средств управления возможности: графический интерфейс, возможность настройки способа визуализации и уровня детализации, отбора отображаемых событий.

Специфичной для средств активного аудита является возможность получения объяснений от анализаторов и решателей по поводу обнаруженной подозрительной активности. Такие объяснения помогают выбрать адекватный способ реагирования.

При формировании классификационной схемы средств активного аудита в [28] предлагается выделить базовый (минимальный) ПЗ, а дополнительные требования компоновать в функциональные пакеты.

Функциональный пакет (ФП) — это неоднократно используемая совокупность функциональных компонентов, объединенных для достижения определенных целей безопасности [8].

ПЗ, соответствующие классам защищенности, строятся на основе базового ПЗ и соответствующих комбинаций ФП.

В [28] предлагается зафиксировать профили для следующих разновидностей средств активного аудита:

- класс 5 — защита одного информационного сервиса с отслеживанием фиксированного набора характеристик и пороговым анализом (базовый ПЗ);
- класс 4 — защита однохостовой конфигурации с произвольным набором информационных сервисов, отслеживанием сетевого трафика, системных и прикладных событий, пороговым и простым сигнатурным анализом в реальном масштабе времени;
- класс 3 — защита сегмента локальной сети от многоэтапных атак при сохранении остальных предположений класса 4;
- класс 2 — защита произвольной конфигурации с выявлением нетипичного поведения при сохранении остальных предположений класса 3;
- класс 1 — наложение всех требований с возможностью обеспечения заданного соотношения между ошибками первого и второго рода.

В контексте «Общих критериев» важным и сложным является поднятый в [28] вопрос о целесообразности разработки и применения жестких классификационных схем для сервисов безопасности. С одной стороны, гибкость требований ОК такова, что на их основе можно разработать множество профилей защиты с минимальными требованиями, учитывающими специфику информационных систем (ИС) и их окружения и позволяющими добиться необходимого уровня безопасности с минимальными затратами. С другой стороны, едва ли не все информационные системы имеют тенденцию к частым и многочисленным изменениям, способным нарушить истинность сделанных в ПЗ предположений безопасности. Слишком точная подгонка профилей защиты (равно как и характеристик ИС) опасна, у них должен быть запас прочности. В приведенной выше классификации предусмотрено изменение защищаемой конфигурации, поэтому у заказчика есть возможность выбрать класс «на вырост».

Далее, классификационная схема показывает способы усиления функций безопасности (для средств активного аудита это в первую очередь расширение спектра отслеживаемых параметров, повышение оперативности и усложнение методов анализа регистрационной информации). Это важно при выборе подходящей реализации сервиса безопасности из большого числа доступных вариантов.

Наконец, наличие большого числа несравнимых между собой минимальных профилей создает проблемы и для производителей сервисов безопасности, поскольку вовлекает их в многочисленные процедуры сертификации. Конечно, при этом могут быть использованы результаты предыдущих испытаний, но у каждой процедуры все равно остается существенная постоянная часть (финансовая и временная).

Можно сделать вывод, что для совокупности профилей защиты целесообразно с самого начала иметь в виду построение иерархии наследования с применением соответствующих функциональных пакетов. Часть узлов в этой иерархии (например, общие требования к сервисам безопасности) могут быть фиктивными в том смысле, что им не соответствуют профили для законченных изделий ИТ, однако они столь же необходимы, как и (обобщенные) интерфейсы в объектно-ориентированных системах.

3.4. Анонимизаторы

Анонимизаторы предназначены для выполнения функциональных требований приватности (класс FPR «Общих критериев»). В данном разделе, основываясь на статье [31] и профиле защиты [32], мы рассмотрим одну из разновидностей анонимизаторов — сеть серверов пересылки, обеспечивающую приватность пользователей электронной почты.

Вероятно, приватность — это единственный класс функциональных требований ОК, направленных не на обеспечение безопасности иерархически организованных, жестко администрируемых систем, а на защиту специфических интересов пользователей информационных сервисов. В «Оранжевой книге» Министерства обороны США и Руководящих документах Гостехкомиссии России подобных требований не было, поэтому опыт по их применению необходимо нарабатывать, что придает работам [31] и [32] особую ценность. Происходит становление так называемой многоаспектной информационной безопасности, когда делается попытка учесть весь спектр интересов (порой конфликтующих между собой) всех субъектов информационных отношений, а также все виды конфигураций ИС, в том числе децентрализованные, не имеющие единого центра управления.

Как известно (см., например, [33]), класс FPR содержит четыре семейства: FPR_ANO (анонимность — возможность совершать действия, не раскрывая идентификационных данных пользователя), FPR_PSE (псевдонимность — анонимность с сохранением подотчетности), FPR_UNL (невозможность ассоциации — анонимность с сокрытием связи между действиями одного пользователя), FPR_UNO (скрытность или ненаблюдаемость —

сокрытие самого факта использования ресурса или услуги).

Псевдонимность полезна, например, когда за активное использование каких-то специфических платных услуг полагаются скидки. Невозможность ассоциации позволяет защититься от раскрытия личности пользователя путем анализа профиля его поведения. Назначение семейств FPR_ANO и FPR_UNO очевидно.

Сеть серверов пересылки почты состоит из независимо администрируемых узлов.

Отправитель определяет путь сообщения в этой сети. Само сообщение шифруется таким образом, что каждому серверу пересылки известны только предыдущий и следующий узлы. В результате достигается невозможность установления ассоциации между отправителем и получателем. Если в сообщении отсутствуют идентификационные данные отправителя, обеспечиваются анонимность, невозможность ассоциации и, отчасти, скрытность. Псевдонимность может быть реализована путем использования особым образом заданных обратных адресов. Отметим, что на тех же принципах могут быть реализованы анонимизаторы для других информационных сервисов, в частности, для Web-доступа. Существуют свободно распространяемые (Mixmaster) и коммерческие (компании Zero Knowledge Systems) реализации сетей серверов пересылки.

На сеть серверов пересылки можно смотреть двояко: изнутри и извне. Традиционный взгляд изнутри, с точки зрения гипотетического администратора сети, обязанного обеспечить ее безопасность и, в частности, высокую доступность, ведет к традиционному же профилю защиты, требования которого противоречат приватности.

Действительно, для защиты сети от атак на доступность необходимо выявлять подозрительную активность путем накопления и анализа регистрационной информации, уметь прослеживать пользователей и т.п. В силу указанных причин в данном разделе мы будем придерживаться взгляда извне, с точки зрения пользователя сервиса анонимизации; с этих позиций и разработан профиль [32].

Для сети серверов пересылки сообщений выделяются следующие специфические угрозы безопасности.

- Возможность установления ассоциации между отправителем и получателем, если путь сообщения проходит только через один сервер пересылки.
- Установление контроля над несколькими серверами пересылки и проведение совместного анализа их регистрационной информации.

Отметим также, что многие общие угрозы (маскарад сервера с целью распространения поддельных криптографических ключей, установление контроля над одним из серверов пересылки с целью извлечения необходимой конфиденциальной информации, перенаправление потоков данных с целью подмены части сети пересылки, анализ потоков данных между пользовательской системой и сетью пересылки и т.п.) приобретают в данном контексте специфический характер, так как направлены на нарушение приватности пользователей.

Формулируются два специфических положения политики безопасности.

- Должна обеспечиваться анонимность сообщений, то есть получатель не может узнать идентификационных данных отправителя, если только последний сам не поместил их в сообщение в явном виде.
- Должна обеспечиваться невозможность прослеживаемости сообщений, то есть в результате перехвата сообщения нельзя одновременно узнать его отправителя и получателя.

Перечислим специфические цели безопасности.

- Серверы пересылки должны принимать и обрабатывать сообщения, не опираясь на какую-либо информацию об отправителе.
- Содержание сообщений на всем пути следования должно быть скрыто от сторонних наблюдателей.
- Сеть серверов пересылки должна быть построена таким образом, чтобы успешно противостоять попыткам анализа потоков данных, в частности, потоков между пользовательской системой и сетью.
- Сеть серверов пересылки должна быть построена таким образом, чтобы пользователь мог (и, более того, был обязан) корректно распределять между узлами сети данные, существенные для невозможности прослеживания адресатов сообщения, а также выбирать узлы, участвующие в обработке сообщения. Сеть пересылки обязана реализовать пользовательский выбор.
- Пользователи и узлы сети пересылки должны однозначно идентифицироваться, а сообщения — доставляться в нужные узлы с сохранением конфиденциальности соответствующих данных.
- Сеть серверов пересылки должна быть построена таким образом, чтобы использование, распространение и интервал времени доступности данных, влияющих на возможность ассоциации пользователей, были минимальными.

- Ни один субъект (пользователь, администратор, злоумышленник) не должен иметь возможность получения информации, достаточной для прослеживания отправителей сообщений.

Специфические цели безопасности для среды:
- узлы сети пересылки должны администрироваться независимо и, более того, антагонистично;
- сеть пересылки должна быть топологически распределенной.

Чтобы лучше понять приведенные ниже специфические функциональные требования, целесообразно помнить, что рассматриваемый профиль защиты сформирован с позиций пользователя, так что в объект оценки (ОО) входят как серверы пересылки, так и клиентские системы. Все потоки данных контролируются функциями безопасности ОО; экспорта или импорта данных не происходит.

В пределах области действия функций безопасности имеют место следующие виды операций:
- передача сообщения клиентской системой серверу пересылки;
- пересылка между серверами сообщений, а также управляющей информации (в том числе ключевой);
- доставка сообщения с сервера на клиентскую систему;
- обработка сервером пересылки (транзитных) сообщений;
- операции, выполняемые сервером с криптографическими ключами: генерация, распространение, хранение, доступ, использование, уничтожение;
- порождение сервером пересылки фиктивных сообщений.

Для отправки сообщения пользователь должен задать целевой адрес и цепочку серверов пересылки. При получении почты требуется аутентификация, так как входящие сообщения нуждаются в расшифровании.

В пределах объекта оценки действует специфическая форма политики принудительного управления доступом, состоящая в том, что каждый элемент пользовательских данных приписывается определенному субъекту, так что только этот субъект получает право на доступ к приписанным ему данным. Далее, провозглашается политика борьбы со скрытыми каналами, чтобы противостоять попыткам анализа потоков данных.

Специфические функциональные требования состоят в следующем.

- Полное управление доступом (FDP_ACC.2). Политика принудительного управления доступом должна распространяться на всех субъектов (серверы пересылки, клиентское ПО, пользователи, администраторы), все объекты (в том числе на содержание и маршрутную информацию сообщений) и все операции.
- Ограниченное управление информационными потоками (FDP_IFC.1). Должна проводиться в жизнь политика борьбы со скрытыми каналами применительно к серверам пересылки, клиентскому ПО, сообщениям, передаче и приему сообщений (FDP_IFC.1.1).
- Частичное устранение неразрешенных информационных потоков (FDP_IFF.4). Должна проводиться в жизнь политика борьбы со скрытыми каналами, чтобы уменьшить до заданных пределов утечку информации о работе пользователей с сетью пересылки, возникающую за счет анализа периферийных потоков данных (FDP_IFF.4.1). Получение профилей поведения компонентов сети пересылки путем анализа периферийных потоков данных должно быть невозможным (FDP_IFF.4.2).
- Полное управление временем хранения данных (FDP_IRC.2). Все объекты, нужные для нормальной работы сети пересылки, должны удаляться сразу после завершения операций с ними. Отметим, что это не просто специфическое, но новое функциональное требование, предложенное автором профиля защиты.
- Управление атрибутами безопасности (FMT_MSA.1). Согласно политике принудительного управления доступом, только пользователь, сгенерировавший данные, может выполнять операции над их атрибутами безопасности, в число которых входят маршрут сообщения и его рандомизация, минимальное число пересылок, число отправляемых избыточных сообщений, параметры потоков данных и криптографических алгоритмов и т.п. (FMT_MSA.1.1).
- Анонимность без запроса информации (FPR_ANO.2). Должны обеспечиваться невозможность определения подлинного имени отправителя сообщения, обрабатываемого сетью серверов пересылки (FPR_ANO.2.1) и непрослеживаемость и анонимность пересылки сообщений для всех пользователей без запроса какой-либо ссылки на подлинное имя пользователя (FPR_ANO.2.2).
- Размещение информационных ресурсов (FPR_TRD.2). Сеть пересылки должна состоять из отдельных взаимодействующих частей, в каждой из которых реализуются свои правила

аутентификации и управления доступом (FPR_TRD.2.1). Доступ к данным другой части должен предоставляться только по явному запросу (FPR_TRD.2.2).

Данные, критичные для невозможности ассоциации (маршрут, время и т.п.), должны храниться в виде, исключающем возможность их полного чтения одной частью сети, чтобы обеспечить невозможность прослеживания всей цепочки между отправителем и получателем сообщения (FPR_TRD.2.3). (Этот и два последующих компонента предложены автором профиля защиты.)

- Распределение обработки сообщений (FPR_TRD.3). По сути этот компонент аналогичен предыдущему с точностью до замены слова «храниться» на «обрабатываться».
- Невозможность ассоциации пользователей (FPR_UNL.2). Должна обеспечиваться невозможность определить, что сообщения были отправлены одним и тем же пользователем.

Для мер доверия безопасности предлагается оценочный уровень 5. Напомним, что его характерными особенностями являются применение формальной модели политики безопасности, полуформальных функциональной спецификации и проекта верхнего уровня с демонстрацией соответствия между ними, а также проведение анализа скрытых каналов разработчиками и оценщиками. Это очень высокий уровень, но в данном случае его выбор представляется оправданным, поскольку, с одной стороны, объект оценки является относительно простым, с легко формализуемой политикой безопасности, а с другой стороны, в функциональных требованиях предусмотрен анализ скрытых каналов.

Рассмотренный профиль защиты, на наш взгляд, является весьма поучительным. Он демонстрирует как достоинства, так и недостатки «Общих критериев». К числу достоинств можно отнести богатый набор современных функциональных требований, особо выделив требования приватности. К сожалению, как мы уже отмечали, эти требования носят «точечный», а не концептуальный или архитектурный характер. Для требования распределенности архитектуры пришлось вводить новое семейство.

Отметим, в свою очередь, что отнесение его к классу приватности не кажется нам оправданным. Распределенность принципиально важна для целого ряда систем, но если в системах электронных платежей, как и в сети серверов пересылки, она действительно является необходимым условием приватности (в профиле новое семейство получило наименование «распределения доверия»), то во многих других случаях она играет инфраструктурную роль, обеспечивая живучесть (устойчивость к отказам) и/или масштабируемость (в сочетании с архитектурой менеджер/агент).

Очевидно, архитектурные требования заслуживают отдельного класса.

Требования безопасности повторного использования, безусловно, должны быть дополнены требованиями минимизации времени хранения объектов, как это и сделано в рассмотренном профиле. Это важно, помимо приватности, практически для всех приложений криптографии, в ситуациях, когда образуются временные файлы с информацией ограниченного доступа и т.п.

Авторы работ [31, 32] справедливо замечают, что введение новых функциональных требований имеет свои оборотные стороны. Конкретные профили получаются проще, естественнее, однако сравнение профилей с нестандартными компонентами усложняется. Возможный выход подсказывает технология программирования, предусматривающая проблемно-ориентированные расширения базовых интерфейсов, как это сделано, например, в Java-системах [34]. Подобные расширения можно разработать и стандартизовать быстрее, чем полный набор требований, поскольку они затрагивают более узкий круг специалистов, объединенных к тому же общностью интересов.

3.5. Выпуск и управление сертификатами

В документе [35] предлагается упорядоченное семейство из четырех профилей защиты для аппаратно-программных компонентов, реализующих выпуск, аннулирование и управление сертификатами открытых ключей (удовлетворяющими, например, спецификациям X.509) (Certificate Issuing and Management Components, CIMC).

Таким образом, перед нами жесткая классификационная схема, рассчитанная на применение в разнообразных средах. Каждый заказчик, учитывая степень критичности ИС и реальные риски, сам выбирает необходимый уровень защищенности и соответствующий ему профиль. На нижнем (первом) уровне потенциал злоумышленников и риски предполагаются низкими, в первую очередь обеспечивается защита от случайных ошибок авторизованных пользователей (например, за счет использования принципа разделения обязанностей). При переходе на более высокие уровни угрозы нарастают, а требования ужесточаются. На верхнем (четвертом) уровне злоумышленниками могут быть и авторизованные пользователи, а требования безопасности оказываются настолько жесткими, что

удовлетворить им могут только перспективные изделия ИТ. Это разумный подход, снабжающий ориентирами и заказчиков, и разработчиков.

Объект оценки в профилях из [35] является элементом инфраструктуры открытых ключей и в общем случае включает следующие функциональные компоненты.

- Центр выпуска и аннулирования сертификатов (именуемый также удостоверяющим центром, УЦ). Это — ядро ОО. Сгенерированная информация помещается в хранилище (см. далее). Между различными УЦ могут существовать отношения доверия.
- Центры приема пользовательских запросов на создание сертификатов или изменение их статуса. Верифицируют представленные пользователем данные. Это также обязательные компоненты объекта оценки.
- Серверы, обслуживающие протокол оперативной выдачи статуса сертификатов. Этот компонент может отсутствовать или находиться за пределами ОО.
- Серверы восстановления и/или распространения секретного ключевого материала. Эта функция также является дополнительной.

Отметим, что хранилище сертификатов и информации об их статусе, обслуживающее запросы приложений, находится вне рамок ОО.

Помимо функциональных, в объект оценки входят следующие инфраструктурные компоненты.

- Криптографический модуль. Он подписывает сертификаты и списки их аннулирования, при необходимости генерирует криптографические ключи. Требования безопасности, предъявляемые к криптографическим модулям, изложены в федеральном стандарте США FIPS PUB 140-2 [36], заменившем FIPS PUB 140-1 (см. [37]).
- Модуль администрирования.
- Модуль идентификации и аутентификации.
- Модуль ролевого управления доступом.
- Модуль протоколирования и аудита.

Представленная выше логическая компонентная архитектура не обязательно совпадает с физической структурой объекта оценки. В принципе возможна монолитная реализация ОО, объединение/расщепление компонентов и т.д.

Переходя к специфическим функциональным требованиям безопасности для среды, отметим выделение в [35] четырех ролей:

- администратора (отвечающего за установку, конфигурирование, обслуживание нужд пользователей и т.п.);
- оператора (отвечающего за резервное копирование и восстановление);
- инспектора (ведающего запросами и утверждением сертификатов и их статуса);
- аудитора (отвечающего за анализ регистрационной информации).

В соответствии с компонентом FMT_SMR.2 (ограничения на роли безопасности), один пользователь не может выступать более чем в одной из перечисленных выше ролей (FMT_SMR.2.3).

Среда должна обеспечить защиту конфиденциальности данных пользователя при передаче между функциями безопасности (FDP_UCT). Более точно должна быть обеспечена базовая конфиденциальность обмена данными (FDP_UCT.1). Аналогичная защита должна обеспечиваться для конфиденциальных данных самой среды (FPT_ITC.1, FPT_ITT.1). Кроме того, требуется контроль целостности данных.

Криптографическими методами должна контролироваться целостность (в частности, аутентичность) программного кода, присутствующего в системе, и кода, который в принципе может быть загружен (дополнительные требования профиля FPT_TST_CIMC.2 и FPT_TST_CIMC.3).

Среди специфических (более того, дополнительных по сравнению с «Общими критериями») функциональных требований безопасности для объекта оценки выделим следующие.

- Инициирование и обработка события подписывания регистрационного журнала (FPT_CIMC_TSP.1). С конфигурируемой периодичностью должно инициироваться названное событие. Подпись должна контролировать целостность по крайней мере тех регистрационных записей, которые появились после предыдущего подписывания. В регистрационной записи о самом событии подписывания должны присутствовать электронная цифровая подпись, значение хэш-функции или имитовставка аналогичного назначения.
- Инициирование и обработка события постановки третьей стороной подписанных меток времени (FPT_CIMC_TSP.2). Этот компонент аналогичен предыдущему и обеспечивает дополнительный контроль целостности регистрационных данных (например, на случай компрометации объекта оценки).
- Резервное копирование и восстановление (FDP_CIMC_BKP.1), с дополнительными (криптографическими) мерами контроля целостности и обеспечения конфиденциальности (FDP_CIMC_BKP.2), с точностью до последней

завершенной транзакции (FDP_CIMC_BKP.3). Эти компоненты направлены на безопасное (в том числе свободное от внедрения вредоносного кода) восстановление. Отметим, что подобные требования полезны также для СУБД и других систем с транзакциями.

- Принудительные доказательство и верификация подлинности источника данных о статусе сертификатов и других данных, критичных для безопасности (FCO_NRO_CIMC.3). Аналогично должны контролироваться заявки на регистрацию сертификатов. Предпочтительным способом доказательства подлинности являются цифровые подписи (FCO_NRO_CIMC.4).
- Экспортируемая информация об изменении статуса сертификатов должна иметь формат, описанный в спецификациях X.509 для списков аннулирования или RFC 2560 для протокола оперативной выдачи статуса сертификатов (FDP_CIMC_CSE.1).
- Защита конфиденциальности секретных ключей пользователей (FDP_ACF_CIMC.2) и функций безопасности (FMT_MTD_CIMC.4). Секретные ключи обслуживающего персонала и функций безопасности объекта оценки должны храниться в стандартном криптографическом модуле или шифроваться стандартными методами. Секретные ключи пользователей должны шифроваться с помощью долговременных ключей защиты. Аналогичные требования предъявляются к хранению секретных ключей симметричных методов шифрования (FDP_ACF_CIMC.3 и FMT_MTD_CIMC.5).
- Секретные ключи должны экспортироваться либо в зашифрованном виде, либо с использованием процедур разделения знаний (FDP_ETC_CIMC.4, FDP_ETC_CIMC.5, FMT_MTD_CIMC.6, FMT_MTD_CIMC.7).
- Контроль целостности хранимых открытых ключей (FDP_DSI_CIMC.3). Открытые ключи, хранимые в объекте оценки вне криптографического модуля, должны быть защищены от несанкционированного изменения стандартными криптографическими методами. Проверка целостности должна производиться при каждом доступе к ключу.
- Обнуление секретных ключей (FCS_CKM_CIMC.5). Функции безопасности должны обеспечить обнуление открытого представления секретных ключей в криптографическом модуле.
- Контроль допустимости значений полей сертификатов (FMT_MOF_CIMC.3). Функции безопасности должны контролировать значения полей сертификатов в соответствии с правилами, заданными администратором. Аналогичные проверки должны производиться для списков аннулированных сертификатов (FMT_MOF_CIMC.5) и сообщений протокола оперативной выдачи статуса сертификатов (FMT_MOF_CIMC.6).
- Генерация сертификатов (FDP_CIMC_CER.1). Должны генерироваться только корректные сертификаты, удовлетворяющие требованиям стандарта (X.509) и правилам, заданным администратором. Аналогичные требования должны выполняться для списков аннулированных сертификатов (FDP_CIMC_CRL.1) и сообщений протокола оперативной выдачи статуса сертификатов (FDP_CIMC_OCSP.1). До выпуска сертификата необходимо убедиться, что его предполагаемый владелец обладает секретным ключом, ассоциированным с открытым ключом из сертификата.

Требования доверия безопасности усиливаются параллельно с возрастанием выбранного уровня профиля защиты. Для верхнего, четвертого уровня используются в основном требования ОУД4 и, частично, ОУД5, а также требование ALC_FLR.3 (систематическое устранение недостатков), не входящее ни в один ОУД.

На наш взгляд, рассмотренное семейство профилей может служить примером при построении классификационных схем в Руководящих документах Гостехкомиссии России.

3.6. Анализ защищенности

Анализ защищенности — сравнительно новый, но весьма популярный сервис безопасности, помогающий реализовать профилактический подход к обеспечению защиты информационных систем. По сути он весьма прост, но «Общими критериями» поддержан крайне слабо. Посмотрим, как можно изменить это положение.

Предлагается ввести новый класс функциональных требований — FPA: анализ защищенности. В нем может быть три семейства.

- FPA_HLP: описание уязвимости, выдача рекомендаций по ее устранению.
- FPA_RAD: автообнаружение контролируемых объектов.
- FPA_SPA: анализ характеристик защищенности.

Семейство FPA_HLP может состоять из одного компонента.

- FPA_HLP.1 — описание, выдача (быть может, с заданным уровнем детализации) сведений об

уязвимостях, содержащихся в базе данных системы анализа защищенности. (Эта база данных аналогична базе правил в компоненте анализа регистрационной информации FAU_SAA.1.).
Семейство FPA_HLP может использоваться многократно (например, для выдачи сведений об атаках средствами активного аудита). Его роль можно сравнить с ролью комментариев в языках программирования; отсутствие подобного семейства, на наш взгляд, является методологической недоработкой авторов «Общих критериев».
Выдача пояснений полезна не только для анализа защищенности, но и для выбора реакции на обнаруженную атаку (почему система анализа решила, что атака имеет место? какие правила при этом сработали? насколько серьезна обнаруженная атака? — на все эти вопросы администратор безопасности должен получить оперативные, информативные ответы).

Семейство FPA_RAD может состоять из одного компонента.

- FPA_RAD.1 — автообнаружение компонентов анализируемой ИС, содержащихся в базе данных системы анализа защищенности.

Семейство FPA_SPA может состоять из трех компонентов.

- FPA_SPA.1 — проверка наличия в системе и/или сети сущностей, указанных в базе данных системы анализа защищенности. (Имеются в виду небезопасные сервисы, такие, например, как TFTP).
- FPA_SPA.2 — анализ характеристик выявленных сущностей (номеров версий, конфигурационных параметров, атрибутов доступа, слабых паролей — и здесь анализируется то, что перечислено в базе данных). Правила для анализа могут быть сложными, охватывающими несколько характеристик.
- FPA_SPA.3 — проверка реакции объекта на выполнение определенных действий (имитация атак, перечисленных в базе).

Можно надеяться, что предлагаемый класс функциональных требований безопасности поможет в разработке профиля защиты для систем анализа защищенности.

4. Специфические требования к комбинациям и приложениям сервисов безопасности

4.1. Операционные системы

Операционные системы (ОС) — классический объект оценки по требованиям безопасности еще со времен «Оранжевой книги». Более того, точка зрения на них как на важнейшее, чуть ли не единственное защитное средство до сих пор остается весьма распространенной. С современных позиций ОС можно рассматривать как комбинацию сервисов идентификации и аутентификации, управления доступом и протоколирования/аудита. Кроме того, операционные системы обеспечивают базовые, инфраструктурные свойства безопасности, такие, как разделение доменов и посредничество при обращениях.

Для операционных систем разработан целый ряд профилей защиты (см. [38-43]). К этой же группе документов можно отнести руководство по разработке профилей для перспективных коммерческих продуктов ИТ [44], поскольку оно, как и [38-41], ориентировано на класс безопасности С2 «Оранжевой книги».

Мы, однако, рассмотрим проект [42] (адаптированный вариант профиля [43]), в целом соответствующий третьему классу защищенности по классификации Гостехкомиссии России для средств вычислительной техники, поскольку он более представителен с точки зрения требований безопасности.

Операционные системы, удовлетворяющие рассматриваемому проекту ПЗ, должны обеспечивать дискреционное и мандатное управление доступом, мандатное управление целостностью, предоставлять криптографические сервисы. Все пользователи должны иметь ассоциированный уровень допуска, определяющий максимальный уровень чувствительности данных, к которым они могут обращаться (см. выше подраздел «Управление доступом»).

Вероятно, единственная специфическая угроза для рассматриваемого класса ОС заключается в неадекватной классификации данных на основе их меток, что предоставляет пользователям возможность осуществлять несанкционированный доступ к (помеченным) данным. В качестве контрмеры формулируется специфическая цель безопасности: «Операционная система должна предостав-

лять возможность расставлять точные метки чувствительности и целостности».

Еще одна очевидная цель состоит в том, что операционная система должна поддерживать домен для своего собственного выполнения, что защитит ее и ее ресурсы от внешнего вмешательства, искажения или несанкционированного раскрытия.

Для борьбы с маскарадом сервера операционная система должна предоставлять средства, предотвращающие связь пользователя с некоторой сущностью, выдающей себя за операционную систему, но не являющейся таковой.

Из числа специфических функциональных требований наибольший интерес представляют криптографические компоненты. Остановимся на них подробнее.

- Генерация криптографических ключей (FCS_CKM.1). Симметричные криптографические ключи должны генерироваться в соответствии с согласованным с ФАПСИ алгоритмом, реализуемым аппаратным или программным генератором случайных чисел (см. далее компонент FCS_COP_EXP.2) и/или схемой генерации ключей, основанной на криптографии с открытым ключом, использующей программный и/или аппаратный генератор случайных чисел, определенный в FCS_COP_EXP.2, с хэш-функцией по ГОСТ Р 34.11-94. Асимметричные криптографические ключи должны генерироваться, согласуясь с параметрами криптографического преобразования, используя генератор случайного числа и/или генератор простых чисел и удовлетворяя ГОСТ Р 34.10-2001 в части генерации простых чисел, ГОСТ Р 34.10-2001 для реализации процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма, ГОСТ 28147-89 для реализации процедур зашифрования и расшифрования данных, а также требованиям из этого проекта ПЗ: FPT_CTST_EXP, FCS_COP_EXP.2 и документации разработчика. Дополнительное требование данного проекта ПЗ состоит в том, что к каждому сгенерированному симметричному ключу должна добавляться имитовставка алгоритма ГОСТ 28147-89 или контрольная сумма другого аттестованного алгоритма (FCS_CKM_EXP.1).
- Распределение криптографических ключей (FCS_CKM.2). Согласно проекту профиля [42], ключи должны распределяться (вручную или автоматически) в соответствии с требованиями ФАПСИ и действующих нормативных документов. Не предусматривается автоматическое распределение секретных ключей асимметричных криптосистем.
- Доступ к криптографическим ключам (FCS_CKM.3). Ключи должны храниться только в зашифрованном виде в соответствии с требованиями ФАПСИ и действующих нормативных документов (FCS_CKM.3.1). Дополнительное требование: не должна храниться информация, позволяющая однозначно идентифицировать ключ (FCS_CKM_EXP.3.1).
- Уничтожение криптографических ключей (FCS_CKM.4). Криптографические ключи должны уничтожаться в соответствии с требованиями ФАПСИ и действующих нормативных документов. Стирание ключей и других критичных параметров должно быть немедленным и полным. Стирание должно быть выполнено так, чтобы поверх ключа/критичной области памяти записывались три или более различных шаблонов (FCS_CKM.4.1).
- Криптографические операции (FCS_COP.1). Операции зашифрования/расшифрования данных должны выполняться в соответствии с алгоритмом криптографического преобразования по ГОСТ 28147-89 или другим аттестованным алгоритмом. Операции вычисления цифровой подписи должны выполняться в соответствии с алгоритмом выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма по ГОСТ Р 34.10-2001 или другим аттестованным алгоритмом. Операции хэширования должны выполняться в соответствии с определенным ГОСТ Р 34.11-94 или другим аттестованным алгоритмом. Операции обмена криптографическими ключами должны выполняться в соответствии с требованиями ФАПСИ и действующих нормативных документов. (FCS_COP.1.1).
- Генерация случайных чисел (FCS_COP_EXP.2 это дополнительный компонент, предложенный в данном проекте ПЗ). Генерация случайных чисел должна выполняться множеством независимых аппаратных и/или программных датчиков, выходы которых объединяются с использованием хэш-функции по ГОСТ Р 34.11-94 или другого аттестованного алгоритма (FCS_COP_EXP.2.1). Датчики случайных/псевдослучайных чисел должны быть защищены от нарушения алгоритмов (режимов) их функционирования (FCS_COP_EXP.2.2).
- Защита остаточной информации криптографического ключа (FDP_RIP_EXP.2 – дополнительный компонент). Любой ресурс, содержащий критичные параметры безопасности, при освобождении этого ресурса должен быть очищен от всей информации путем перезапи-

си поверх его содержимого, как определено процедурой уничтожения ключа.

- Отделение домена функций безопасности (FPT_SEP_EXP.1 – дополнительный компонент). Должен поддерживаться криптографический домен, отделенный от остальных функций безопасности, защищенный от вмешательства и искажения недоверенными субъектами (FPT_SEP_EXP.1.1).
- Тестирование криптографического модуля (FPT_CTST_EXP – дополнительное семейство). Для проверки правильности функционирования криптографического модуля необходимо реализовывать возможность его тестирования путем выполнения набора встроенных тестов при начальном запуске, по запросу администратора по криптографии и периодически (FPT_CTST_EXP.1.1). Тесты должны обеспечивать проверку и документирование статистических характеристик генераторов случайных/псевдослучайных чисел и отображение результатов тестирования (FPT_CTST_EXP.1.2). Должны выполняться тесты обнаружения ошибок в ключе при начальном запуске и по запросу администратора по криптографии (FPT_CTST_EXP.1.3). Должно выполняться самотестирование каждого компонента, участвующего в генерации ключей, немедленно после генерации ключа для верификации их функционирования в соответствии с FCS_CKM.1.1 и FCS_COP_EXP.2 (FPT_CTST_EXP.1.4). Сгенерированный ключ не должен использоваться, если самотестирование какого-либо компонента завершилось неудачей (FPT_CTST_EXP.1.5).
- Доверенный маршрут (FTP_TRP_EXP.1 – дополнительный компонент). Криптографический модуль должен обеспечивать маршрут связи между собой и локальными пользователями, который логически отличим от других маршрутов и предоставляет уверенную идентификацию самого себя (FTP_TRP_EXP.1.1).

Для обслуживания криптографических средств в рассматриваемом проекте ПЗ предусмотрен также дополнительный компонент требований доверия безопасности.

- Анализ скрытых каналов криптографического модуля (AVA_CCA_EXP.1). Для криптографического модуля разработчик должен провести поиск скрытых каналов утечки критичных параметров безопасности (AVA_CCA_EXP.1.1D). Разработчик должен представить документацию анализа скрытых каналов (AVA_CCA_EXP.1.2D).

Документация анализа должна идентифицировать скрытые каналы в криптографическом модуле и содержать оценку их пропускной способности (AVA_CCA_EXP.1.1C).

Документация анализа должна содержать описание процедур, используемых для заключения о существовании скрытых каналов в криптографическом модуле, и информацию, необходимую для проведения анализа скрытых каналов (AVA_CCA_EXP.1.2C). Документация анализа должна содержать описание всех предположений, сделанных в процессе анализа скрытых каналов (AVA_CCA_EXP.1.3C).

Документация анализа должна содержать описание метода, используемого для оценки пропускной способности канала для случая наиболее опасного сценария (AVA_CCA_EXP.1.4C). Документация анализа должна содержать описание наиболее опасного сценария использования каждого идентифицированного скрытого канала (AVA_CCA_EXP.1.5C). Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств (AVA_CCA_EXP.1.1E). Оценщик должен подтвердить, что результаты анализа скрытых каналов показывают, что криптографический модуль удовлетворяет функциональным требованиям (AVA_CCA_EXP.1.2E). Оценщик должен выборочно подтвердить правильность результатов анализа скрытых каналов, применяя тестирование (AVA_CCA_EXP.1.3E).

Можно видеть, что в проекте профиля [42] вопросы криптографии изложены весьма пространно, однако смысл всех требований предельно прост: соответствие национальным стандартам (их три) и требованиям ФАПСИ. На наш взгляд, целесообразно выделить требования к криптографическим модулям в отдельный документ, как это сделано в федеральном стандарте США FIPS PUB 140-2 [36], а не перегружать ими профиль защиты ОС.

Еще одна специфическая особенность ОС – возможность управления использованием ресурсов, их распределением между пользователями. Для этого уместно применить механизм квотирования.

- Максимальные квоты (FRU_RSA.1). Должны задаваться выделяемые пользователям квоты долговременной и оперативной памяти, а также процессорного времени (FRU_RSA.1.1).

Рассмотренный проект профиля защиты для операционных систем показывает, как важно соблюдать определенный уровень формализации изложения, а также единый уровень детализации. Неоднородность ПЗ чревата несистематичностью, завышением или занижением требований. К сожа-

лению «Общие критерии» не регламентируют этот аспект разработки профилей защиты, заданий по безопасности и функциональных пакетов.

Отдельного рассмотрения заслуживают специфические функциональные требования, присутствующие в проекте [38]. Выше, в разделе «Системы активного аудита», мы отмечали важность требований к интерфейсам и их безопасности. В [38] предложен дополнительный элемент FAU_GEN.1-CSPP.3, предписывающий предоставление прикладного программного интерфейса для добавления собственных данных к общему регистрационному журналу и/или для ведения приложениями собственных журналов.

Для управления экспортом данных пользователя в соответствии с политикой безопасности введен элемент FDP_ETC.1-CSPP.3, предусматривающий выделение отдельного пула выходных каналов (например, путем резервирования номеров TCP-портов), недоступных обычным приложениям.

Для поддержки распределенных конфигураций предлагается целый ряд дополнительных требований, направленных на обеспечение конфиденциальности (FPT_ITC.1.1-CSPP), целостности (FPT_ITI.1.1-CSPP), согласованности (FPT_SYN-CSPP.1.1) критичных данных функций безопасности.

В заключение этого подраздела следует отметить, что в Центре безопасности информации разработан проект базового профиля защиты для ОС и разрабатывается профиль защиты ОС в средах, требующих высокую робастность (защищенность), с тем, чтобы иметь завершенное семейство профилей защиты операционных систем.

4.2. Системы управления базами данных

Системы управления базами данных (СУБД), как и операционные системы, содержат комбинацию сервисов безопасности, однако, в отличие от ОС, не являются самодостаточными. СУБД используют механизмы и функции ОС, и такая двухуровневость ведет к появлению специфических угроз и, соответственно, требует привлечения соответствующих средств противодействия. Например, базы данных располагаются в файлах или на дисках, управляемых ОС; следовательно, к объектам БД можно обратиться как штатными средствами СУБД, так и с помощью механизмов ОС, получив доступ к файлу или устройству. Подобные возможности должны учитываться в профиле защиты для СУБД.

Дальнейшее изложение основано на проекте ПЗ [45] (его прототип [46] соответствует классу безопасности С2 «Оранжевой книги»).

В проекте вводится понятие аутентификационного пакета, который предоставляет для СУБД механизм подтверждения подлинности заявляемого идентификатора пользователя.

В рассматриваемом проекте профиля защиты для этого должен использоваться по крайней мере один из двух механизмов: внешний (аутентификация средствами ОС) или внутренний (аутентификация средствами СУБД).

Еще одним проявлением упомянутой выше двухуровневости является предположение безопасности базовой конфигурации, состоящее в том, что базовая система (операционная система и/или сетевые сервисы безопасности и/или специальное программное обеспечение) установлены, сконфигурированы и управляются безопасным образом.

Аналогичную направленность имеют цели безопасности для среды, предусматривающие, что базовая система должна обеспечить механизмы управления доступом, которые позволят защитить от несанкционированного доступа все связанные с СУБД файлы. Кроме того, ОС должна предоставить средства для изоляции функций безопасности и защиты процессов СУБД.

Отметим, что в распределенной среде управление доступом и изоляция могут обеспечиваться не только средствами базовой ОС, но и архитектурно, путем разнесения компонентов СУБД по узлам сети и использования межсетевых экранов.

Эта возможность в проекте [45] не рассматривается.

Переходя к функциональным требованиям безопасности, укажем на важность требований согласованности данных между функциями безопасности (FPT_TDC), а также согласованности данных функций безопасности при дублировании в пределах распределенного объекта оценки (FPT_TRC). Согласованность может достигаться с помощью некоторой формы обработки распределенных транзакций или путем обновления дублируемых данных с использованием какого-либо протокола синхронизации. К сожалению, требования этих семейств в проекте [45] не представлены, равно как и требования распределенности хранения и обработки для повышения устойчивости к отказам. Конечно, в «Оранжевой книге» ничего подобного не было, однако в наше время, как показывает профиль [32], следование определенным архитектурным принципам является обязательным.

Для защиты от атак на доступность в рассматриваемом проекте предусмотрены реализация квот, выделяемых пользователям (FRU_RSA.1), а также базовые ограничения на параллельные сеансы (FTA_MCS.1).

В целом, на наш взгляд, при доработке проекта [45] необходимо учесть специфику современных СУБД, в частности, требования обеспечения динамической целостности данных, реализуемые механизмом транзакций. Требования безопасного восстановления носят слишком общий характер. Защита от стандартных угроз, существующих в сетевой среде, целиком переложена на базовую систему. Не учтены специфические для СУБД угрозы, описанные, например, в главе «Информационная безопасность систем управления базами данных» книги [47].

4.3. Виртуальные частные сети

Комбинация туннелирования и шифрования (наряду с необходимой криптографической инфраструктурой) на выделенных шлюзах и экранирования на маршрутизаторах поставщиков сетевых услуг (для разделения пространств «своих» и «чужих» сетевых адресов в духе виртуальных локальных сетей) позволяет реализовать такое важное в современных условиях защитное средство, как виртуальные частные сети. Подобные сети, наложенные обычно поверх Интернет, существенно дешевле и гораздо безопаснее, чем действительно собственные сети организации, построенные на выделенных каналах. Коммуникации на всем их протяжении физически защитить невозможно, поэтому лучше изначально исходить из предположения об уязвимости и соответственно обеспечивать защиту. Современные протоколы, поддерживающие спецификации IPsec (см., например, [48]), позволяют сделать это.

Концами туннелей, реализующих виртуальные частные сети, целесообразно сделать межсетевые экраны, обслуживающие подключение организаций к внешним сетям. В таком случае туннелирование и шифрование становятся дополнительными преобразованиями, выполняемыми в процессе фильтрации потоков данных наряду с трансляцией адресов. Помимо корпоративных межсетевых экранов, концами туннелей могут быть мобильные компьютеры сотрудников (точнее их персональные МЭ). Далее соответствующие узлы сети мы будем называть опорными.

В качестве основы последующего изложения выбран проект профиля защиты [49]. В нем объектом оценки является совокупность опорных узлов. Требования к перспективным средствам аналогичного назначения представлены в документе [50].

Поскольку реализация виртуальных частных сетей в значительной степени основывается на криптографических механизмах, в число специфических угроз входят применение злоумышленником методов и средств криптографического анализа, а также компрометация криптографических ключей. Упомянем и угрозы доступности каналов связи.

Для нейтрализации угроз должны быть выполнены функциональные требования безопасности, относящиеся к криптографии. Должен осуществляться контроль доступа к криптографическим ключам (FCS_CKM.3.1), осуществляться шифрование информации, передаваемой в рамках доверенного канала (FCS_COP.1.1), применяться механизмы контроля целостности информации, передаваемой в рамках доверенного канала (FCS_COP.1.1).

В рамках виртуальной частной сети должно осуществляться ограниченное управление информационными потоками (FDP_IFC.1.1). Вообще говоря, через опорные узлы проходят не только потоки данных, предназначенные для виртуальной частной сети, но и данные для внешних адресатов. Эти потоки должны различаться и обрабатываться по-разному (например, первые необходимо шифровать, а вторые — нет). По сути здесь должно быть реализовано межсетевое экранирование, только одна из сетей является виртуальной.

От виртуальных частных сетей требуется реализация некоторых аспектов приватности. Они должны обеспечить, чтобы внешние пользователи не могли определить подлинное имя пользователя, связанного с передаваемой в рамках доверенного канала информацией (FPR_ANO.1.1). В то же время у администратора должна быть возможность наблюдения за использованием ресурсов и функционированием процессов (FPR_UNO.4.1).

Опорные узлы должны обладать определенной отказоустойчивостью, обеспечивая возврат к безопасному состоянию, генерацию записи журнала аудита, сигнализацию администратору, когда происходит сбой в системе электропитания или нарушение безопасности (FRU_FLT.1.1).

Таковы специфические функциональные требования безопасности для виртуальных частных сетей. В «Общих критериях» в явном виде не представлены требования к туннелированию; нет их и в рассмотренном проекте. Возможно туннелирование трактуется лишь как механизм обеспечения анонимности.

4.4. Виртуальные локальные сети

Под виртуальной локальной сетью в проекте профиля защиты [51] понимается такое логическое объединение узлов локальной сети, при котором обмен данными на канальном уровне эталонной семиуровневой модели возможен только между этими узлами.

Использование виртуальных локальных сетей позволяет:

- повысить производительность (и доступность) сети за счет локализации потоков данных;
- обеспечить защиту передаваемых данных посредством логического разделения среды передачи;
- реализовать управление доступом пользователей к сетевым ресурсам.

Разграничение потоков данных обеспечивается путем фильтрации кадров данных.

Таким образом, объект оценки по сути оказывается межсетевым экраном канального уровня.

В проекте [51] рассматриваются следующие варианты построения виртуальных локальных сетей.

- Группировка портов объекта оценки. В этом случае каждый такой порт поддерживает только одну виртуальную сеть.
- Использование специальной метрики для определения принадлежности к конкретной виртуальной локальной сети.

Впрочем, предлагаемые в проекте требования безопасности в равной степени применимы к обоим вариантам.

От рассмотренных ранее межсетевых экранов объект оценки отличается ограниченностью ресурсов и меньшей функциональностью. В частности, вся работа с регистрационной информацией (начиная с хранения) возлагается на среду, точнее на так называемое средство анализа событий. Это освобождает объект оценки от ряда стандартных требований протоколирования и аудита, но ведет к необходимости организации доверенного канала.

4.5. Смарт-карты

Профиль защиты для смарт-карт [52] интересен необычностью объекта оценки. Он позволяет оценить гибкость и разнообразие требований «Общих критериев».

Необычность смарт-карт как объекта оценки заключается в следующем:

- минимум аппаратных ресурсов (интегральная схема, включающая процессор, оперативная и постоянная память относительно небольшого объема, порты ввода/вывода) в сочетании с программным обеспечением ограниченной функциональности (в профиле [52] рассматривается базовое ПО);
- принадлежность неконтролируемой среде, когда держатель карты может являться злоумышленником, располагающим специальным оборудованием.

В защите (обеспечении конфиденциальности и целостности) нуждаются хранящиеся на карте пользовательские данные, программное обеспечение (прикладное и базовое), а также аппаратные компоненты.

Отметим, что приемное устройство, снабжающее смарт-карту электропитанием и связью с внешним миром, не входит в объект оценки.

Учитывая ограниченность ресурсов и потенциально враждебную среду, сервисы безопасности для смарт-карт должны быть отобраны и реализованы с особой тщательностью.

Предположения безопасности для среды состоят в данном случае в следующем.

- После того, как с приемным устройством установлен доверенный канал, оно предполагается достаточно безопасным, чтобы поддерживать доверенные коммуникации.
- Предполагается, что обеспечена конфиденциальность и целостность информации, хранящейся вне карты и существенной для ее безопасности. Имеются в виду как пользовательские данные, так и криптографические ключи, загружаемые приложения и т.п.

С большинством возможных угроз смарт-карта должна справляться самостоятельно, без помощи среды. Выделяются следующие специфические (а также специфически реализуемые и отражаемые) угрозы.

- Осуществление доступа к смарт-карте с использованием специального оборудования, когда преследуется цель выяснить определенные аппаратные и/или программные характеристики (применяемые криптографические механизмы, используемые ключи, хранимые данные и программы и т.п.). Возможны и попытки изменить аппаратно-программную конфигурацию и/или данные, а также попытки перевести смарт-карту в небезопасное состояние, поместив ее в стрессовые условия (например, температурные или электромагнитные).
- Логические атаки: отслеживание зависимостей между входными данными операций, выполняемых смарт-картой, и результатами, попытки перевести карту в небезопасное состояние искусственно инициированным сбросом, использование некорректных входных данных, воспроизведение данных аутентификации, переборные атаки (на криптографические компоненты), попытки загрузки вредоносных программ. К этой же категории угроз можно отнести попытки организовать нештатное взаимодействие прикладных функций и использование возможностей (например, отла-

дочных), предусмотренных для особых этапов жизненного цикла смарт-карты. Одновременное проведение нескольких атак.
- Несанкционированный доступ: попытки злоупотребления полномочиями при доступе к пользовательским данным или данным функций безопасности, попытки использования новой, не до конца оформленной смарт-карты.
- Попытки выявления и анализа утечек информации во время нормальной работы смарт-карты, совместный анализ результатов многих наблюдений.
- Попытки изготовления копий (клонирование) компонентов смарт-карты с целью детального изучения их поведения.

Для среды специфической является угроза замены интегральной схемы, установленной в смарт-карте, с целью несанкционированного доступа к данным пользователя или функций безопасности.

Из специфических положений политики безопасности отметим прежде всего наличие уникальных идентификационных данных для каждого объекта оценки, а также (как ни странно) накопление регистрационной информации, которое необходимо производить, несмотря на ограниченность ресурсов. Аудит может производиться во время сервисного обслуживания смарт-карты.

Как обычно цели безопасности формулируются таким образом, чтобы обеспечить нейтрализацию угроз и выполнить положения политики безопасности. В частности, интегральная схема должна работать в любых, в том числе стрессовых, условиях, должна обеспечиваться защита от многократного использования ресурсов при переборных атаках, изучение передаваемых данных не должно давать дополнительной информации по сравнению с анализом содержимого памяти, нормальное (безопасное) состояние должно устанавливаться сразу после подачи питания или сброса, при замене интегральной схемы на карте обязательно должны оставаться следы и т.п.

Перейдем к рассмотрению специфических функциональных требований.
- Автоматическая реакция аудита безопасности (FAU_ARP) при обнаружении возможного нарушения безопасности. Реакция должна иметь минимальные необратимые последствия. Подчеркнем, что в силу специфики объекта оценки оперативное информирование администратора безопасности в общем случае невозможно; с опасностью приходится бороться самостоятельно.
- Генерация списка регистрационных данных (FAU_LST — дополнительное семейство). На интегральной схеме, устанавливаемой в смарт-карте, нет часов; время поступает только от приемного устройства, которое не считается доверенным. Следовательно, события можно лишь упорядочить по мере их появления, но с ними нельзя ассоциировать дату и время. В регистрационную информацию должны включаться идентификационные данные аппаратных и программных компонентов.
- Противодействие физическому нападению (FPT_PHP.3). Функции безопасности должны противодействовать попыткам эксплуатации в стрессовых условиях, отслеживанию информации, другим физическим атакам, реагируя автоматически таким образом, чтобы предотвратить нарушение политики безопасности (FPT_PHP.3.1).
- Надежное восстановление (FPT_RCV). Автоматическое восстановление без недопустимой потери (FPT_RCV.3), восстановление функции (FPT_RCV.4).

Для требований доверия безопасности в [52] используется усиленный оценочный уровень 4. Усиление обеспечивают компоненты AVA_VLA.3 (систематический поиск уязвимостей, обеспечение стойкости к нападениям, выполняемым нарушителем с умеренным потенциалом) и ADV_INT.1 (модульность).

Важным достоинством работы [52] является выделение двух функциональных пакетов: для интегральной схемы и базового ПО. Эти части могут разрабатываться независимыми производителями, поэтому целесообразно дать им возможность независимой же сертификации, оставив за интегратором (производителем смарт-карт) выбор поставщиков и интегральную сертификацию. В части функциональных требований пакет для базового ПО аналогичен рассмотренному профилю; к аппаратуре предъявляется меньшее число требований. Например, в функциональном пакете для интегральной схемы отсутствуют компоненты FAU_SAA.1 (анализ потенциального нарушения) и FPT_RPL.1 (обнаружение повторного использования), что представляется вполне естественным.

5. Заключение

«Общие критерии» — исключительно мощное, гибкое средство разработки требований безопасности для изделий информационных технологий. В частности, как показывает настоящий обзор, могут быть выделены общие требования к сервисам безопасности, а также учтена специфика конкретных сервисов, фигурирующих по отдельности или в различных комбинациях.

В то же время, сама гибкость «Общих критериев» является источником сложных проблем, в первую очередь относящихся к методологии разработки профилей защиты.

Можно провести аналогию с языками и технологией программирования, когда владение передовым языком программирования вовсе не означает умения проектировать и создавать большие программные комплексы.

Вопросы технологии «программирования» профилей защиты носят разнообразный характер и затрагивают все этапы жизненного цикла ПЗ. Какой подход выбрать при разработке ПЗ: «снизу вверх» или «сверху вниз»? Сами «Общие критерии», имеющие библиотечную (не объектную) структуру, подталкивают к применению подхода «снизу вверх», от отдельных требований к общей функциональности. Однако, как показывает опыт разработчиков профиля [32] и других (равно как и технология программирования), предпочтительным является подход «сверху вниз», от требуемой функциональности объекта оценки к базовым механизмам безопасности.

Еще один технологический аспект — модульность ПЗ. Выделение функциональных пакетов для составных частей объекта оценки, реализованное в работе [52], дает больше свободы и разработчикам, и интеграторам, способствует раннему выявлению и устранению проблем, облегчает работу оценщиков.

Следующий вопрос касается технологии сопровождения множества профилей защиты.

Как соотносить между собой отдельные ПЗ? Как группировать их, выстраивать иерархии и т.п.? Пока зарегистрированных профилей относительно немного (что само по себе является проблемой, но, можно надеяться, временной), очевидно, что их число будет расти, они станут поступать из разных источников, из разных стран, так что поддержание международного статуса «Общих критериев», несомненно, потребует специальных усилий, которые целесообразно планировать заранее.

Очень серьезной проблемой является неполнота функциональных требований «Общих критериев». Как показывают рассмотренные профили, авторам ПЗ приходится добавлять собственные нестандартные классы, семейства, компоненты и элементы, что ведет к несопоставимости разрабатываемых профилей, к усложнению процедур сертификации и взаимного признания сертификатов.

Принципиальным недостатком является отсутствие в «Общих критериях» архитектурных и технологических требований. Такие свойства, как распределенность архитектуры, следование подходу менеджер/агент и т.п., являются необходимыми для успешной реализации функций объекта оценки, они критичны для его безопасности.

Таким образом, проведенный анализ позволяет наметить следующие направления дальнейших исследований и разработок:

- создание новых профилей защиты, охватывающих, по крайней мере, все сервисы безопасности;
- разработка методологии и соответствующих инструментальных средств создания ПЗ;
- разработка дисциплины и инструментальных средств для работы с множеством профилей защиты;
- развитие «Общих критериев», разработка новых стандартных требований безопасности, как «точечных», так и концептуальных, архитектурных;
- разработка дисциплины введения новых нестандартных требований с минимизацией проблем несопоставимости получающихся профилей защиты.

Для решения сформулированных проблем необходима совместная работа специалистов, независимо от их национальной и, тем более, ведомственной принадлежности.

6. Литература

1. Information technology — Security techniques — Evaluation criteria for IT security -Part 1: Introduction and general model. — ISO/IEC 15408-1.1999.
2. Information technology — Security techniques — Evaluation criteria for IT security -Part 2: Security functional requirements. — ISO/IEC 15408-2.1999.

3. Information technology — Security techniques — Evaluation criteria for IT security -Part 3: Security assurance requirements. — ISO/IEC 15408-3.1999.
4. ГОСТ Р ИСО/МЭК 15408-1-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. — М.: ИПК Издательство стандартов, 2002.
5. ГОСТ Р ИСО/МЭК 15408-2-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. — М.: ИПК Издательство стандартов, 2002.
6. ГОСТ Р ИСО/МЭК 15408-3-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. — М.: ИПК Издательство стандартов, 2002.
7. Гостехкомиссия России. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. — Москва, 2002.
8. Information technology — Security techniques — Guide for Production of Protection Profiles and Security Targets. Version. 0.9. — ISO/IEC PDTR 15446, January 4, 2000.
9. Гостехкомиссия России. Руководство по разработке профилей защиты и заданий по безопасности (проект). — Москва, 2002.
10. Гостехкомиссия России. Руководящий документ. Руководство по регистрации профилей защиты (проект). — Москва, 2002.
11. Web-сервер с материалами по «Общим критериям». — http://www.commoncriteria.org/.
12. «Общие критерии» на сервере Национального института стандартов США. — http://csrc.nist.gov/cc/.
13. Бетелин В.Б., Галатенко В.А. Информационная (компьютерная) безопасность с точки зрения технологии программирования. — Труды 4-й Ежегодной конференции консорциума ПрМ «Построение стратегического сообщества через образование и науку». — М.: МГУ им. М.В. Ломоносова, 2001, с. 38-44.
14. Безопасность информационных технологий. Контролируемый доступ. Профиль защиты (первая редакция). — Центр безопасности информации, 2002.
15. Controlled Access Protection Profile. Version 1.d. — U.S. Information Systems Security Organization. U.S. National Security Agency, 8 October 1999.
16. Department of Defense Trusted Computer System Evaliation Criteria. — DoD 5200.28-STD, 1985.
17. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. — Москва, 1992.
18. Безопасность информационных технологий. Меточная защита. Профиль защиты (первая редакция). — Центр безопасности информации, 2002.
19. Labeled Security Protection Profile. Version 1.b. — U.S. Information Systems Security Organization. U.S. National Security Agency, 8 October 1999.
20. Reynolds J., Chandramouli R. Role-Based Access Control Protection Profile Version 1.0 — July 30, 1998.
21. Rational for RBAC Protection Profile. Version 1.0 — July 30, 1998.
22. Jansen W., Walsh J. Draft U.S. Government Application-Level Firewall Protection Profile for Low-Risk Environments. Version 1.b. — September, 1998.
23. Jansen W., Walsh J., Dolan K., Wright P. Final U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments. Version 1.1. — April, 1998.
24. Dolan K., Wright P., Montequin R., Mayer B., Gilmore L., Hall C. Final U.S Department of Defense Traffic-Filter Firewall Protection Profile For Medium Robustness Environments. Version 1.4. — U.S. National Security Agency, May 1, 2000.
25. Профиль защиты для межсетевых экранов корпоративного уровня. — Инфосистемы Джет, 2002.
26. Профиль защиты для межсетевых экранов провайдерского уровня. — Инфосистемы Джет, 2002.
27. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. — Москва, 1997.
28. Бетелин В.Б., Галатенко А.В., Галатенко В.А., Кобзарь М.Т., Сидак А.А. Классификация средств активного аудита в терминах «Общих критериев». — В сб. «Информационная безопасность. Инструментальные средства программирования. Базы данных» под ред. чл.-корр. РАН В.Б. Бетелина.-М.: НИИСИ РАН, 2001, с. 4-26.
29. Intrusion Detection System Analyser Protection Profile. Draft 3. — U.S. National Security Agency. Science Applications International Corporation. Center for Information Security Technology, September 15, 2000.
30. Intrusion Detection System Sensor Protection Profile. Draft 3. — U.S. National Security Agency.

Science Applications International Corporation. Center for Information Security Technology, September 15, 2000.
31. Rannenberg K., Iachello G. Protection Profiles for Remailer Mixes — Do the New Evaluation Criteria Help? — Proceedings of the 16th Annual Computer Security Applications Conference (ACSAC'00). — IEEE Press, 2000, pp. 107-118.
32. Iachello G. User-Oriented Protection Profile for Unobservable Message Delivery using MIX networks, Revision 2.4. — June 6, 1999. http://www.iig.uni-freiburg.de/~giac/User_MIX_PP.pdf.
33. Трубачев А.П., Долинин М.Ю., Кобзарь М.Т., Сидак А.А., Сороковиков В.И. Оценка безопасности информационных технологий. Под общей редакцией В.А. Галатенко. — М.: СИП РИА, 2001. — 356 с.
34. Таранов А., Цишевский В. Java в три года. — Jet Info, 1998, 11-12.
35. Lee A., et. al. Certificate Issuing and Management Components Family of Protection Profiles. Version 1.0. — U.S. National Security Agency, October 31, 2001.
36. FIPS PUB 140-2: Security Requirements for Cryptographic Modules. — U.S. Department of Commerce, NIST, May, 25, 2001.
37. Cryptographic Module Validation Program. — http://csrc.nist.gov/cryptval/.
38. Stoneburner G. CSPP-OS — COTS Security Protection Profile — Operating Systems. Draft Version 0.4. — U.S. Department of Commerce, NIST, February 5, 2001.
39. Stoneburner G. Rationale for CSPP — COTS Security Protection Profile — Operating Systems. Draft Version 0.4. — U.S. Department of Commerce, NIST, February 5, 2001.
40. Безопасность информационных технологий. Одноуровневые операционные системы в средах, требующих среднюю робастность. Профиль защиты (вторая редакция). — Центр безопасности информации, 2002.
41. Protection Profile For Single-level Operating Systems In Environments Requiring Medium Robustness. Version 1.22. — Information Systems Assurance Directorate. U.S. National Security Agency, 23 May 2001.
42. Безопасность информационных технологий. Многоуровневые операционные системы в средах, требующих среднюю робастность. Профиль защиты (вторая редакция). — Центр безопасности информации, 2002.
43. Protection Profile for Multilevel Operation Systems in Environments Requiring Medium Robustness. Version 1.22. — Information Systems Assurance Directorate. U.S. National Security Agency, 23 May 2001.
44. Stoneburner G. CSPP — Guidance for COTS Security Protection Profiles. Version 1.0. NISTIR 6462. — U.S. Department of Commerce, NIST, December, 1999.
45. Безопасность информационных технологий. Система управления базой данных. Профиль защиты (первая редакция). — Центр безопасности информации, 2002.
46. Database Management System Protection Profile. Version 2.1. — May, 2000.
47. Галатенко В.А. Информационная безопасность — практический подход. Под ред. В.Б. Бетелина. — М.: Наука, 1998. — 301 с.
48. Галатенко В., Макстенек М., Трифаленков И. Сетевые протоколы нового поколения. — Jet Info, 1998, 7-8.
49. Средства построения виртуальных частных вычислительных сетей. Защита от несанкционированного доступа к информации. Базовый профиль защиты (проект, редакция 01). — МИФИ, 2002.
50. Sheridan M., Sohmer E., Varnum R. A Goal VPN Protection Profile For Protecting Sensitive Information. Release 2.0. — U.S. National Security Agency, 10 July, 2000.
51. Средства построения виртуальных локальных вычислительных сетей. Защита от несанкционированного доступа к информации. Базовый профиль защиты (проект, редакция 01). — МИФИ, 2002.
52. Smart Card Protection Profile (SCSUG-SCPP). Version 3.0. — Smart Card Security User Group, 9 September 2001.

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается с 1995 года
Издатель: компания Джет Инфо Паблишер

Главный редактор: Дмитриев В.Ю. *(vlad@jet.msk.su)*
Технический редактор: Овчинникова Г.Ю. *(galya@jet.msk.su)*
Россия, 127006, Москва, Краснопролетарская, 6
тел. (095) 972 11 82, 972 13 32
факс (095) 972 07 91
email: JetInfo@jet.msk.su http://www.jetinfo.ru

Подписной индекс по каталогу Роспечати 32555